SENTINEL

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

D1.3 The SENTINEL experimentation protocol

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 1**
Deliverable Title	The SENTINEL experimentation protocol
Version	4.0
Date of Submission	30/11/2021
Main Editor(s)	Evangelia Kavakli (IDIR), Peri Loucopoulos (IDIR), Yannis Skourtis (IDIR)
Contributor(s)	Argyrios Alexopoulos (FP), Christos Dimou (ITML), Manolis Falelakis (INTRA), Daryl Holkham (TIG), Eleni-Maria Kalogeraki (FP), Zoe Kasapi (CECL), Christopher Konialis (CG), Tatiana Trantidou (ITML), Philippe Valoggia (LIST)
Reviewer(s)	Eleftheria Marini (ITML), Philippe Valoggia (LIST)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	04/10/2021	Draft	Confidential
2.0	29/10/2021	Draft	Confidential
3.0	09/11/2021	Draft	Confidential
4.0	14/11/2021	Internal Review	Public
5.0	29/11/2021	Final	Public

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
CCPA	California Consumer Privacy Act
CS	Cybersecurity
DIH	Digital Innovation Hub
DPO	Data Protection Officer
EMA	Exome Management Application
GA	Grant Agreement
GDPR	General Data Protection Regulation
KPI	Key Performance Indicator
KR	Key Result
LGPD	Lei Geral de Proteção de Dados
MTBF	Mean time between failures
MTTF	Mean time to failure
MTTR	Mean time to repair
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PCI DSS	Payment Card Industry Data Security Standards
PDP	Personal Data Protection
PTC	Project Technical Committee
R&I	Research and Innovation
RIS3	Regional research and Innovation strategy for Smart Specialisation
ROCOF	Rate of occurrence of failure
V&V	Verification and Validation
WCAG	Web Content Accessibility Guidelines

Executive Summary

Deliverable D1.3 reports on a preliminary version of the SENTINEL experimentation protocol that will be further refined and finalised, in line with the Grant Agreement (GA), in WP6 and according to end-users' requirements, in their engagement in real life demonstrators, thus providing detailed validation and evaluation of the SENTINEL platform. Furthermore, this deliverable is aligned with the work of tasks T1.1 and T1.2. Task T1.1 investigated the SME challenges and requirements with respect to Cybersecurity (CS) and Personal Data Protection (PDP), which were reported in Section 2 of deliverable D1.1 "The SENTINEL baseline", whereas task T1.2 defined the architecture of the SENTINEL platform, as reported in deliverable D1.2 "The SENTINEL technical architecture".

Regarding this preliminary version of the experimentation protocol we:

- define the experimentation process (phases and steps);
- discuss the conditions for accessibility of participants in the actual experiments;
- identify relevant standards and benchmarks;
- define the verification indicators and juxtapose these to the SENTINEL platform, as detailed in D1.2;
- define the validation indicators to be used in the experiments involving the pilot cases, as detailed in D1.1;
- define the instruments (templates) to be used when the experiments are carried out and results are reported.

The overall assessment of the SENTINEL outcomes will be an ongoing process, following the project progress. This assessment will use the Key Performance Indicators (KPIs) and Key Results (KRs) defined in the GA which will be continuously monitored and revised, beginning with the work of task T1.3 as reported in this deliverable.

1 Introduction

A significant concept within systems engineering is the verification and validation (V&V) process, during which the effectiveness of the system under development is measured through some suitable metrics and by providing some evidences (ISO/IEC/IEEE, 2015).

In particular, ***verification*** is a set of activities that compares a system or a system element against required characteristics. These include the specified functional requirements as well as quality characteristics that relate to (a) the system usage (quality in use), e.g., effectiveness, efficiency, user satisfaction, etc., and (b) product quality properties, e.g., performance efficiency, reliability, security, maintainability, etc. The main goal of verification is to ensure quality of the system under development and may include a number of experimental tests obtained on system components as well as on the integrated system by utilising a number of tools such as simulations, performance tests, benchmarks and prototypes.

Validation is a set of activities ensuring and gaining confidence that a system is able to accomplish its use, goals, and objectives in the intended operational environment (Walden, Roedler et al., 2015). Validation, investigates the system acceptability by its intended users and is usually performed on the whole system (Brusa, Calà et al., 2018). In particular, validation aims to obtain experimental evidence on the implemented system. Different experimental strategies may be used at different stages of system development. In the early stages, surveys might be used to collect information from user representatives off-line, usually through a presentation of the candidate solution in joint workshops. At later stages validation becomes more dynamic whereby the operational solution is studied using a case study or controlled experiment approach (Wohlin, Runeson et al., 2012).

1.1 Purpose of the Document

The purpose of this document is to report on the results produced from work that was carried out in task T1.3 whose aims according to the GA are to:

(i) define access control rights, accessibility and all relevant technical, organisational, legal (GDPR) and commercial aspects of allowing SENTINEL consortium to execute the demonstrations
(ii) define industrial challenges and requirements that the solution needs to address
(iii) identify dependent and independent verification and validation variables for the demonstrations, both for the SMEs that are part of the consortium, and for the ones to be reached via Digital Innovation Hubs
(iv) define a concrete and coherent demonstration plan, consistent with WP6 activities
(v) introduce scientific and industry-validated benchmarks and standards (T7.3) for all SENTINEL associated technologies identified in T1.2
(vi) use them to demonstrate significant and measurable enhancements in parameters of privacy-by-design processes in SMEs' environments
(vii) perform a revision of R&I, Business and Dissemination KPIs
(viii) define a verification and validation methodology to evaluate SENTINEL offerings.

1.2 Structure of the Document

This document is structured in such a way so as to address the aims of task T1.3, outlined in Section 1.1, in a systematic way. The overarching aim of T1.3 is in describing the experimentation process for verifying the functionality and quality of the SENTINEL digital platform and for validating the results of the project in terms of methodology and software tools against the needs of SME stakeholders. To this end, the work of T1.3 has been aligned with the work in other tasks in order to ensure consistency across project activities and results. Referring to the aims outlined in Section 1.1: (a) aim (i) was informed by the work carried out in T8.1 and reported in deliverable D8.9, in which a data management plan has been outlined together with the process of accessing the data for verification, re-use, curation and preservation; (b) aim (ii) is reported in D1.1, in which the industrial challenges and requirements of SMEs are outlined; (c) aim (iii) has been informed by work in T1.2, in which the components of the SENTINEL architecture that need to be evaluated as part of the experimentation process, are defined.

The SENTINEL experimentation process is described in Section 2 and comprises the experimentation cycle, the principles for the participation procedure to be followed, the verification and validation variables as criteria for evaluation and the relevant benchmarks and standards upon which these variables are defined. Section 2 introduces two templates used for the capture of actual evaluation variables; one dedicated to verification and the other to validation elicitation process. These templates were used by the SENTINEL project stakeholders to define the variables relevant to either the development of technologies or to the use of these technologies (see Section 4 for details).

Given that SENTINEL results will be applied, tested and evaluated through 3 pilot cases, it is important to establish at the outset the context of the experimentation process and this is done in Section 3, in which each pilot case is described.

The verification variables are detailed, using the dedicated template, introduced in Section 2.3, to fill in all the information related to the SENTINEL platform assets, by the asset owners or developers. These details are presented in Section 4. Similarly, the validation variables are detailed in a dedicated template in Section 5, completed by the SME stakeholders of the pilot cases.

The objectives of the project overall are to be evaluated for their attainment through an analysis of Key project Results (KRs), as defined in the GA, which are measured through Key Performance Indicators (KPIs). KRs and KPIs are presented in Appendices A and B. For each verification and validation variable, we have included a correspondence between the variable and KRs in the tables of Sections 4 and 5 and a reflective discussion on this is given in Section 0.

Finally, Section **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** concludes this document with a summary of contributions from the work of task T1.3, a reflection on these contributions and a discussion on the way that the results from this work will be utilised in subsequent phases of the project.

1.3 Intended readership

This document is intended for both consortium members and external to the project stakeholders.

Consortium members involved in the implementation of the SENTINEL digital platform have defined, for each asset for which they are involved in its development, the quality variables and corresponding metrics, against which these assets will be evaluated.

Consortium members involved in the pilot cases have defined, for each pilot case, the validation variables and corresponding metrics, along the two domains of ‘business’ and ‘Cybersecurity (CS) and Personal Data Protection (PDP)’, against which the experimentation process, using the pilot cases, will be carried out in work-package 6.

Stakeholders, external to the project, will be informed on the way in which SENTINEL intends to systematically evaluate its technical solutions in assisting SMEs deal with their CS for privacy needs. This will be especially beneficial in Work Package 7, during the dissemination and communication phase of the project.

2 The SENTINEL experimentation process

2.1 The experimentation lifecycle

The SENTINEL experimentation aims at evaluating and validating the SENTINEL digital framework architecture and its implementation in the specific project pilot cases. The SENTINEL experimentation process follows the basic steps that must be performed in any empirical study (Wohlin, Runeson et al., 2012). To this end, the experimentation lifecycle (depicted in Figure 1) consists of:

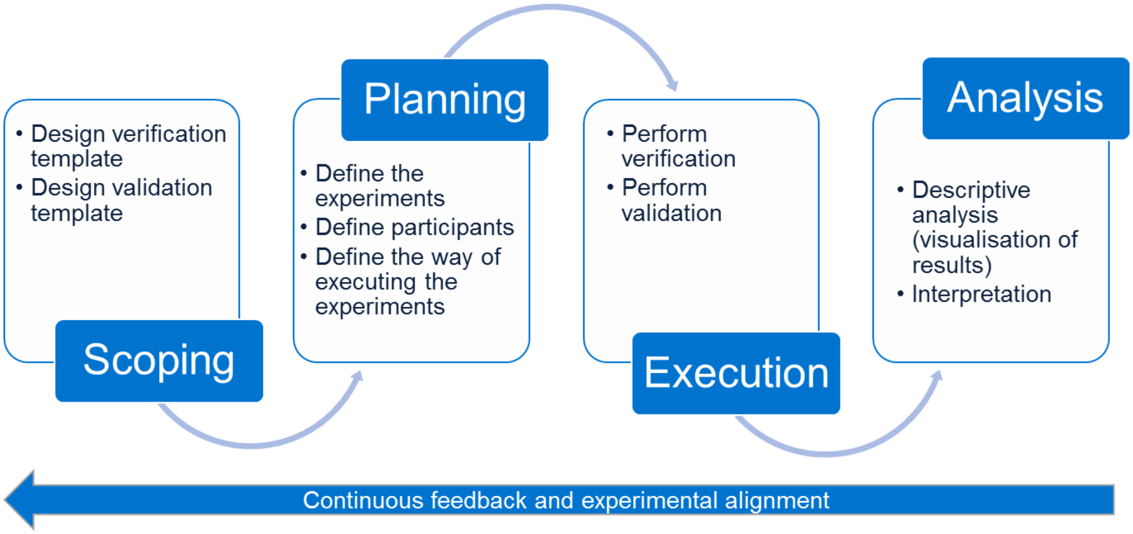
Scoping
• Design verification template
• Design validation template
Planning
• Define the experiments
• Define participants
• Define the way of executing the experiments
Execution
• Perform verification
• Perform validation
Analysis
• Descriptive analysis (visualisation of results)
• Interpretation
Continuous feedback and experimental alignment

Figure 1. The SENTINEL experimentation process

- Two **definition** phases namely those of *scoping* and *planning* of the experiments in terms of defining the context of the experiments (goals, tasks, participants), as well as identifying the business and technology variables to be measured. In addition, applicable benchmarks as well as business improvements sought are identified in these initial phases.
- Two **operational** phases namely those of *execution* and *analysis*, which focus on the implementation of the real-life experiments and the quantitative and qualitative evaluation of the SENTINEL platform at component, system and experiment level.

A main characteristic of the experimental process is that it considers both technical and business requirements, aiming to evaluate not only the performance of the SENTINEL platform, but also its alignment with the needs of the SME end users. We refer to these two complementary tasks as verification and validation respectively. The main verification stakeholders are the technology providers, whilst validation stakeholders are the SME users. Therefore, the experimentation process requires the collaboration of both technology and SME stakeholders in all phases.

Another important aspect is that it is an iterative and incremental process, whereby the definition of the experiments is iteratively refined to increased level of certainty in order to reflect (a) revisions of the pilot cases definitions and associated requirements and (b) progress in the design of the SENTINEL digital framework and associated technology characteristics. This is referred to as 'experimental alignment' and aims to ensure that the designed experiments reflect the actual business and technical requirements.

2.1.1 Scoping

The aim of this first step is to scope verification and validation and gain insight with respect to the experimentation objectives, i.e., what we wish to measure and why. To this end, it includes the initial definition of (a) the technology variables to be used for evaluating the system quality and (b) the experiments to be performed for assessing the achievement of the SME objectives[1]. The former takes into consideration existing quality assurance and testing standards. The latter, adapts the experiment template suggested in (Basili and Rombach, 1988), whereby each experiment can be expressed in terms of the following aspects: <Goal(s) of experiment>, <Quality focus > and <Context>. Table 1 summarises these aspects.

In more detail, the ***goal*** of the experiment refers to the object and purpose of the experiment. The ***object*** is the entity that is studied in the experiment. In SENTINEL experiments the object of study is the SENTINEL platform, but it could also be a specific SENTINEL function or sub-component. The ***purpose*** defines what the intention of the experiment is. It may be for example, to evaluate the impact on specific enterprise capabilities. The ***quality focus*** is the primary effect under study in the experiment. Quality focus refers to the specific variables that will measured, be effectiveness, cost, etc. The ***context*** is the 'environment' in which the experiment is run. The context briefly defines which personnel is involved in the experiment (subjects) and the experiment workflow, i.e., the type and order of activities that will be involved in each experiment.

Table 1. Experiment overview

Experiment name	
Experiment's Goal(s)	*Object, purpose*
Experiment's Variables	*Quality focus*
Experiment Workflow	*Context*
Participants	*Context*

During the scoping phase the focus is mainly on determining the goal(s) and quality focus of the experiments, while the context details will be determined during the subsequent planning phase (see Section 2.1.2).

2.1.2 Planning

Whilst scoping is where the foundation for the experiments is laid, planning is where the design of the experiments is determined. This includes choosing suitable instrumentation (i.e., measuring and reporting mechanisms for each quality variable) and the specification of the type and order of activities (workflow) to be performed by the experimental subjects and develop guidelines if necessary and define measurement procedures. In addition to measuring mechanism, baseline values and improvements sought are also defined at this stage.

[1] Such objectives have been defined in the baseline phase (see deliverable D1.1).

2.1.3 Execution

After the experiments have been designed and planned, they must be carried out in order to collect the measurements that should be analysed. This comprises the *execution phase*. As already mentioned, execution consists of two complementary tasks namely, verification and validation. Verification evaluates the performance of the SENTINEL platform in parts and as a whole and is conducted by technology providers, using appropriate testing procedures and applicable benchmarks. During validation, the SENTINEL platform is presented to the SME subjects. Validation consists of three steps: (a) *preparation*, where subjects are chosen and data to be used are prepared, (b) *execution*, where the subjects perform their tasks according to the experimental workflow and measurements are collected, and (c) *reporting*, where the collected measurements are recorded using the chosen instruments.

2.1.4 Analysis

Finally, in the analysis phase the evaluation concludes with the interpretation and the reporting of results by coming to a consensus about them with all stakeholders involved. Quantitative analysis may be carried out using, for example, descriptive statistics. Appropriate benchmarks are used to compare and interpret the results obtained during the project (see Section 2.4).

2.2 Execution procedure

During the execution phase (see Section 2.1.3), special attention should be paid to the appropriate provision of information to the data subjects involved in the project activities, as well as to the categories of data which will be processed. Participants must be informed about the purposes of processing and their consent should be explicitly given.

The data processed in the SENTINEL pilot activities will be subject to access control rights due to organisational, legal (GDPR) and commercial considerations. An appropriate procedure will be established to ensure that pilots can be implemented effectively, while the relevant legal and regulatory framework is complied with.

To achieve this, the processing of personal data must be based on one of the lawful bases for processing set out in Articles 5 and 6 GDPR. These principles are: (i) lawfulness (personal data must be obtained in a lawful and fair manner); (ii)transparency (the data subject must know whether and which personal data are being held about him or her); (iii) data minimisation (personal data must be adequate, relevant and no more than is necessary for the purpose justifying their processing); (iv) time limitation (personal data cannot be kept longer than necessary); (v) accuracy (personal data must be accurate and regularly updated) and (vi) integrity (taking appropriate technical and organisational security measures in order to avoid unauthorised access, changes, leaks of personal data and accidental loss, destruction, damage).

Data anonymisation should be sought out as an alternative to processing personal data whenever feasible and appropriate for the attainment of the project’s goals. Anonymisation can be achieved through the following techniques: data masking (disclosure of data with modified values, e.g., letters are replaced by the “*” character); pseudonymisation (replacement of true identifiers of specific persons with false ones, a.k.a. pseudonyms, e.g., changing the data subject’s name and/or other identifiers to render them non-identifiable); generalisation (excluding certain data in order to render the data subject non-identifiable, e.g., their last name); data swapping (shuffling dataset attribute values); data perturbation (modifying the initial dataset marginally by applying round-numbering methods and adding random noise; only appropriate for large data sets); synthetic data (algorithmically generated information with no relation to any actual case, through the construction of mathematical models based on patterns contained in the original dataset). The appropriate data anonymisation technique will be selected for each relevant pilot activity based on the particular characteristics of the data sets which are going to be processed, in order to ensure data privacy is maintained and all related risks of data breaches are minimised.

2.3 Eliciting and representing experimentation variables

To assist the experimentation process, two templates have been designed:

- A **verification template** (see Section 2.3.1), focusing on the evaluation of the technical quality of the SENTINEL platform in parts and as a whole using appropriate quality variables and associated metrics.
- A **validation template** (see Section 2.3.2), focusing on the empirical evaluation of the SENTINEL platform in real SME settings and against business specific indicators.

During the scoping and planning phases these templates are used to elicit and represent experimentation variables and associated metrics and baseline values. In fact, the templates together with the variables and metrics defined in Sections 2.3.1 and 2.3.2, should be treated as pre-defined lists that can be further refined and adjusted to the context of each technology component / experiment by removing irrelevant variables or by adding new ones where applicable.

The resulting templates during the execution phases will be used as questionnaires in order to collect and record actual measurements.

2.3.1 Verification template

The SENTINEL verification template shown in Table 2 aims to assist the assessment of the quality of the SENTINEL platform in parts and as a whole, trying to answer the following questions:

- What is the object of the verification (asset name)?
- Which quality aspects will be verified (verification variable)?
- How do we measure each quality aspect (metric)?
- What are the current baselines/benchmarks and what is the expected improvements, when applicable (baseline value, benchmark, expected result)?
- To which project KR does the verification correspond (Relevant KRs)?

Table 2. The SENTINEL verification template

Asset name	Verification variable	Metric	Baseline value	Benchmark	Expected result	Relevant KRs

Depending on the object of the verification, the **asset name** might refer to specific SENTINEL plugins (e.g., Security Infusion, IdMS, MITIGATE), major building blocks (contexts) of the SENTINEL technological framework (e.g., MySentinel, Self-assessment, Observatory), or the integrated SENTINEL platform. The **verification variable** corresponds to asset quality properties that we wish to assess. These are based on the ISO/IEC 25010:2011 (ISO/IEC, 2011b) standard for software systems quality focusing on a product quality model which categorises product quality properties into eight characteristics: functional suitability, reliability, performance efficiency, usability, security, compatibility, maintainability and portability. Each characteristic is composed of a set of related sub-characteristics shown in Table 3.

Table 3. Verification variables according to (ISO/IEC, 2011b) product quality characteristics and sub-characteristics

Verification variable	Sub-variables	Relevant Metrics
Functional suitability: degree to which a product or system provides functions that meet stated and implied needs when used under specified conditions.	Functional completeness Functional correctness Functional appropriateness	No of requirements implemented No of requirements tested % of requirements tested successfully
Performance efficiency: performance relative to the number of resources used under stated conditions.	Time behaviour Capacity	Response time Requests per second Wait time Average load time Concurrent users Throughput CPU utilisation Memory utilisation
Usability: degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.	Appropriateness recognisability Learnability Operability User error protection User interface aesthetics Accessibility	Task completion rate Number of errors User ratings
Reliability: degree to which a system, product or component performs specified functions under specified conditions for a specified period of time.	Maturity Availability Fault tolerance Recoverability	Mean time between failures (MTBF) Mean time to failure (MTTF); Mean time to repair (MTTR); Rate of occurrence of failure ROCOF)
Security: degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorisation.	Confidentiality Integrity Non-repudiation Accountability Authenticity	% of security requirements tested successfully Resilience

For each verification variable, a set of quantifiable **metrics** should be defined, whose measurement relates to the achievement (or not), of a specific variable. For example, in the case of performance efficiency, relevant metrics include response time, throughput, concurrent users, CPU utilisation, etc. In the case of functional suitability, a relevant metric might be the number of requirements that have been implemented.

Baseline refers to a metric value that forms the base of the verification. It is used to compare the results obtained against historical system results or the results of the previous system in place. **Benchmark** is used to verify the obtained values against industry standards (see Section 2.4). The expected improvements (with respect to the baseline and benchmark testing, where applicable) are listed in the column **Expected result**.

The verification process will also seek to prove that the key project results (see Appendix B) are met. We have juxtaposed the verification variables on these expected key results and this is indicated in the last column of Table 2 (**Relevant KRs**).

Technology providers can refine and adjust the verification template in order to define the variables that will be used to verify their technology contribution and define applicable metrics baseline values and benchmarks (as described in Section 3).

2.3.2 Validation template

The validation template shown in Table 4 is meant to be used for defining the quality focus of the experiments. It has a similar structure to the verification template, only now the focus is on user-oriented quality indicators defined at the ***business*** and ***CS and PDP*** level. Filling this template answers the following questions:

- How do you validate the impact on the business objectives and on the CS and PDP related objectives (validation variable)?
- What metrics (objective and subjective) can be used to measure this impact (metric)?
- What are the current baselines/situation and what is the expected improvements, when applicable (baseline value, benchmark, expected result)?
- Who are the subjects involved in the evaluation e.g., business managers, software developers, DPO, security officers, staff, etc. (evaluators)?
- To which project KR does the validation correspond (Relevant KRs)?

Table 4. SENTINEL validation template

	Validation variable	Metric	Baseline value	Benchmark	Expected result	Evaluators	Relevant KRs
Business							
CS & PDP							

At the business level **validation variables** and associated **metrics** draw on existing research regarding business KPIs and metrics used for assessing the effectiveness of innovative technology solutions.

For example, based on an extended study regarding the indicators used to evaluates software ecosystems (Fotrousi, Fricker et al., 2014) the quality variables that can be used for validating that a software system meets the business objective fall into the following categories:

- **Diversity** includes attributes to measure heterogeneity and openness for such heterogeneity.
- **Financial** includes attributes to measure economic aspects such as investment, cost, and price.
- **Satisfaction** includes attributes to measure satisfaction and the related concepts of suitability, interestingness, learnability, usability, accessibility, acceptability, trust, and reputation.
- **Performance** includes attributes to measure performance, including resource utilization, efficiency, accuracy, and effectiveness.
- **Freedom from risk** includes attributes to measure the ability to avoid or mitigate risks and includes the related concerns of security, reliability, maturity, availability, and other related guarantees.
- **Compatibility** includes attributes to measure the degree to which an entity can perform well in a given context, interoperate or exchange information with other entities, and be ported from one context to another one.
- **Maintainability** includes attributes to measure flexibility, respectively the ability to be changed.

Furthermore, in the DataBench project (DataBench Consortium, 2019) seven quality indicators have been selected as the most relevant for measuring the impacts of innovative technology investments on business performance, on the basis of business literature and research of technology vendors and users. These are shown in Table 5.

Table 5. Validation variables and associated metrics for measuring the impact of innovative technology investments on business performance (DataBench Consortium, 2019)

Business validation variable	Proposed Metric
Revenues increase: Increase in company revenues thanks to the adoption of technology.	Absolute value: % increase
Profit increase: Increase in company profit thanks to the adoption of technology.	
Cost reduction: Reduction in process costs thanks to the introduction of technology.	
Time efficiency: Efficient use of time in business processes: This is often used as a simple proxy for productivity improvements.	Average subject rating on a scale from 1 to 5
Product/Service quality: Product/Service features corresponding to users' implied or stated needs and impacting their satisfaction.	
Customer satisfaction: A measure of customers' positive or negative feeling about a product or service compared with their expectations.	
Business model innovation: Novel ways of mediating between companies' product and economic value creation.	

With respect to CS and PDP effectiveness a number of studies exist that focus on key variables and associated metrics as shown in Table 6 (Ponemon Institute, 2010) (Jaquith, 2007; Hewitt, 2021).

Table 6. CS and PDP validation variables and associated metrics

CS and PDP validation variable	Proposed Metric
Uptime: The ability to avoid business disruption caused by CS and PDP incidents.	• Time to incident detection • Time to incident resolution • Incident workload
Compliance: The ability to achieve compliance with all applicable regulations and laws.	• Results of privacy internal audits • On time regulator notification • Increased awareness of regulatory frameworks • No of new organizational measures/procedures enacted • No of PDP-related trainings attended by staff / year
Threat containment: The ability to prevent or quickly detect external threats.	• Security risks detected • Security risks mitigated
Cost efficiency: The ability to manage investments in information security and data protection in a competent manner.	• Cost of technologies • CS and privacy investment • ROI
Data breach prevention: The ability to prevent or detect internal threats.	• No of incidents detected • No of incidents prevented • No of incidents resolved

Baseline values can be defined for comparing obtained results to agreed values. For example, with respect to GDPR compliance and in particular the results of privacy internal audits the baseline consists of the following:

- Comprehensive and updated Data Protection Policy in place.
- Informed consent procedures applied (incl. information notices, consent forms, procedures for the exercise of data subject's rights).
- Appropriate organizational/security measures in place, equivalent to the ISO/IEC 27001:2013 standard (ISO/IEC, 2013).
- Appropriate protocols enacted on data minimization, including anonymization techniques.

Similarly, **benchmarks** can be used to verify the obtained values against industry standards (see Section 2.4.3). During the initial phases of the experimental protocol, business users can refine and adjust this validation template in order to define and detail the scope of each experiment.

The expected improvements (with respect to the baseline and relevant benchmarks, where applicable) are listed in the column **Expected result**. The experiments will be performed by subjects referred to in Table 4 as **Evaluators**. These might include business experts, IT security experts, DPOs, etc. As in the case of verification, the validation process will also seek to evaluate the fitness of the SENTINEL offerings as defined in the related key project results (column **Relevant KRs** in Table 4).

The experiments identified and which will be used in WP6 are detailed in Section 5.

2.4 Relevant benchmarks and standards

The experimentation process and the defined verification and validation variables defined in Section 2.3 are consistent with existing standards and benchmarks, which are discussed in Sections 2.4.1, 2.4.2 and 2.4.3. This will ensure a high level of objectivity during the analysis process, thus satisfying KR-5.1 namely that "*all SENTINEL solutions, products and services aligned and harmonised with regulations and EU standards*".

Three types of benchmarks are used: ***technology***, ***user experience*** and ***business***. The technology and user experience benchmarks relate to the verification variables discussed in Section 2.3.1, while the business benchmarks relate to the validation variables presented in Section 2.3.2.

2.4.1 Technology benchmarks and standards

Information security and privacy standards have been drafted and are being proposed to support SMEs towards integrating best practices into their procedures and mitigate risks that may disrupt business continuity and cause monetary, reputational, as well as other types of losses. Towards this direction, ENISA has published a set of recommendations (ENISA, 2015b; ENISA, 2015a; ENISA, 2016) on increasing the adoption of relevant standards, which targets a variety of stakeholders, ranging from EU and Member States policy makers to standards developing organisations, large and small businesses. The following aspects are identified as key barriers responsible for the limited uptake of standards by SMEs in ENISA's report:

- **Lack of awareness** of applicable standards by SMEs that may assist them mitigate technology risks. The majority of SMEs are only familiar with a limited number of standards (e.g., GDPR, the ISO/IEC 27000 series). However, various regulatory standards include many more than these; for example, the Payment Card Industry Data Security Standards (PCI DSS) apply to SMEs that store, process or transmit cardholder and customer/personal data.
- **Lack of resources** that is required by SMEs for standards implementation, which would be otherwise allocated into business activities.
- **Wrongful perception by SMEs** that cyberthreats are mainly targeting large enterprises.
- **Limited EU or international privacy standards** designed to assist SMEs towards ensuring appropriate protection of personal data. Organisations yet do not have enough guidance on which specific controls they should implement to ensure compliance with personal data protection laws. Apart from the ISO/IEC 29100:2011 (ISO/IEC, 2011a) and the CEN CWA 16113:2010 (CWA, 2010), which provide a general privacy framework, there are limited EU or international standards for assisting especially small organisations towards ensuring appropriate personal data protection.
- **Lack of harmonised certification procedures and standards** in robust SME/ME-specific infrastructures.
- **Lack of interoperable solutions (technical standards) and practices (process standards)** affecting the firm, cost-effective and flexible business operations.

In alignment with ENISA's proposed recommendations, SENTINEL works towards:

- increasing familiarisation of SMEs with the standards that they can apply; this is achieved by (i) raising general awareness on the benefits of the SENTINEL framework and (ii) increasing SME engagement and building an ecosystem of stakeholders around SENTINEL offerings;

- driving adoption and compliance through the provision of mechanisms for regulatory compliance; this is achieved by providing maturity rating (RAISE score) and a security assurance and certification platform;
- rendering standards more easily deployable by considering the SMEs specific characteristics; this is achieved by tailored-made recommendations and policy drafting based on the self-assessment of participating SMEs;
- increasing cybersecurity capabilities of SMEs to make them more ready for standard adoption; this is achieved by creating ownership of the information security and data protection functions through providing hands-on simulation and training (via the Cyber Range platform) with a focus on threats to personal data and privacy;
- fostering a common strategy among various stakeholders for improving information security and privacy standardisation for SMEs; this is achieved by promoting international, EU and national collaboration within the context of the project implementation and beyond (ecosystem building) and through the SENTINEL observatory, containing the central knowledge base of SENTINEL including actionable security policies.

SENTINEL aims to create sound links and affect a number of information security, data protection and privacy, business continuity management, incident management, as well as risk management (see Table 7). A more detailed description of the project's standardisation activities will be included as part of deliverable D7.5 "*Exploitation strategy, standardisation activities and best practices*" (due in M18 and M36).

Table 7. List of cross-industry standards and legal frameworks relevant to SENTINEL

Information Security related standards
ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems — Overview and vocabulary
ISO/IEC 27001:2013 Information security management systems - Requirements
ISO/IEC 27002:2013 Code of practice for information security controls
ISO/IEC 27003: 2017 Information technology - Security techniques - Information security management systems-Guidance
ISO/IEC 27004:2016 Information technology - Security techniques - Information security management-Monitoring, measurement, analysis and evaluation
ISO/IEC TR 27016:2014 Information technology - Security techniques - Information security management –Organizational economics
ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity
ISO/IEC 27033 (1-5) Network Security
ISO/IEC TR 20004:2015 Information Technology-Security Techniques-Refining Software Vulnerability Analysis Under ISO/IEC 15408 And ISO/IEC 18045
ISO/IEC 15408:2009 Information technology - Security techniques - Evaluation criteria for IT security
ISO/IEC 15443:2012 Information technology - Security techniques - Security assurance framework
ISO/IEC 15446:2017 Information technology - Security techniques - Guidance for the production of protection profiles and security target
ISO/IEC 19790:2012 Information technology - Security techniques - Security requirements for cryptographic modules
ISO/IEC 19791:2010 Information technology - Security techniques - Security assessment of operational systems
ISO/IEC 23643:2020 Software and systems engineering – Capabilities of software safety and security verification tools
ISO/IEC 19792:2009 Information technology - Security technique - Security evaluation of biometrics
CSA Cloud Controls Matrix

PCI Data Security Standard
Data Protection and Privacy
General Data Protection Regulation GDPR 2016/679
ISO/IEC 29100:2011 Privacy framework
ISO/IEC 29101:2018 Privacy architecture framework
BSI BS 10012:2009 Data protection. Specification for a personal information management system
CEN CWA 16113:2010 Personal Data Protection Good Practices
Business Continuity Management
ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
ISO 22301:2019 Security and resilience-Business continuity management systems-Requirements
ISO 22313:2020 Guidance on Business continuity management systems
Incident management
ISO/IEC 27035:2016-2021 (1-4) Information security incident management and guidelines
ISO/IEC 27037:2012 Security techniques
ISO/PAS 22399:2007 Societal Security
Risk management
ISO/IEC 27005:2018 Information Security Risk Management
ISO 31000:2018 Risk Management
ISO/TR 31004:2013 Guidance of Risk Management
IEC 31010:2019 Risk Management-Risk assessment techniques

Relevant benchmarks, frameworks and software as a service solutions are presented in Table 8. Software as a service solutions are included in this Table since they can be used to compare SENTINEL and its components with existing business solutions.

Table 8. List of technical benchmarks relevant to SENTINEL

Benchmarks		
BenchCouncil benchmarks The International Open Benchmarking Council, BenchCouncil[2], is a non-profit benchmarking organisation, which aims to promote multi-disciplinary benchmarking research and practice and foster collaboration and interaction between industry and academia. BenchCouncil is a new initiative since 2018 with a Chinese foundation and elements of US participation with a plan for further international participation recruitment.		
AIBench	Type	Benchmarking suite
	Description	AIBench is a benchmarking suite that abstracts real-world application scenarios into AI Scenario, Training, Inference, Micro and Synthetics Benchmarks across Datacenter, HPC, IoT, and Edge.
	Metrics	Precision, recall, accuracy, latency
	Reference	https://www.benchcouncil.org/aibench/
	SENTINEL dimension	AI for implementing the “Intelligence for Compliance” notion, i.e., the Intelligent Recommendation Engine
TCP benchmarks The Transaction Processing Performance Council (TPC) is a non-profit corporation operating as an industry consortium of vendors that define transaction processing, database, and Big Data system benchmarks.		
TPCx-AI	Type	Benchmarking suite

[2] https://www.benchcouncil.org/

	Description	TPCx-AI is an end-to-end AI benchmark that is nearing the end of its development in the TPC. The benchmark measures the performance of an end-to-end machine learning or data science platform. The benchmark development has focused on emulating the behaviour of representative industry AI solutions that are relevant in current production data centres and cloud environments. This includes data management, pre-processing, training, scoring as well as serving phases.
	Metrics	Performance of end-to-end data platforms
	Reference	http://tpc.org/tpcx-ai/default5.asp
	SENTINEL dimension	Performance of the Intelligent Recommendation Engine
TPCx-DS	Type	Benchmarking suite
	Description	It is a decision support benchmark that models several generally applicable aspects of a decision support system, including queries and data maintenance
	Metrics	Query response time, query throughput.
	Reference	http://www.tpc.org/tpcds/
	SENTINEL dimension	General performance over queries on top of the SENTINEL Observatory.
2B Advice PrIME 2B Advice PrIME Benchmark Features can determine which privacy measures you need to have in place (based on the privacy measure database) and track your alignment with this benchmark over time. Generate graphical overviews of this progression or view a more detailed list that shows exactly when each privacy measure went into place and how it affected your performance (as compared to the benchmark).		
2B Advice PrIME	Type	Software as a service
	Description	2B Advice PrIME is a web-based data privacy software & management solution that consolidates all the elements of an effective data protection & privacy program into one, streamlined system. 2B Advice PrIME leads the way in cloud-based compliance and data privacy management software with a rich set of features and tools that makes managing a privacy program simple and efficient. From documenting data flows to training your staff, from performing privacy impact assessments to running privacy audits, 2B Advice PrIME makes everything a snap.
	Metrics	---
	Reference	https://www.2b-advice.com/en/data-privacy-software
	SENTINEL dimension	Data protection assessment tools & services
ISF Benchmark The ISF Benchmark results are available in real time – as soon as you submit your data you can view results and begin your analysis and peer comparisons. This confidential initiative allows you to compare your performance against similar anonymous organisations around the world, as well as against six internationally recognized standards. The ISF Benchmark is updated every two years to align with the latest thinking in information security and to provide organisations with improved user experiences and added value		
The ISF benchmark	Type	Benchmark
	Description	The ISF Benchmark Executive Summary provides an easy to digest illustrative overview of how organisations can effectively use the ISF Benchmark to assess and improve their security arrangements. At a time when organisations are being asked to demonstrate their

		resilience to cyber threats by government, suppliers and customers alike, the ISF Benchmark provides that objective analysis allowing you to measure both the effectiveness and value of your security investments
	Metrics	From SOGP 2020, NIST Cybersecurity Framework, CIS Top 20 Critical Security Controls for Effective Cyber Defence, PCI DSS version 3.1, ISO/IEC 27002: 2013 and COBIT 5 for Information Security
	Reference	https://www.securityforum.org/solutions-and-insights/the-isf-benchmark-and-benchmark-as-a-service
	SENTINEL dimension	Data protection
NIST Privacy Framework This voluntary NIST Privacy Framework is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction. Using a common approach—adaptable to any organization's role(s) in the data processing ecosystem—the Privacy Framework's purpose is to help organizations manage privacy risks by: • Taking privacy into account as they design and deploy systems, products, and services that affect individuals; • Communicating about their privacy practices; and Encouraging cross-organizational workforce collaboration—for example, among executives, legal, and information technology (IT)—through the development of Profiles, selection of Tiers, and achievement of outcomes.		
NIST Privacy Framework	Type	Framework
	Description	The NIST Privacy Framework is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy.
	Metrics	Cybersecurity Risks, Privacy Risks, Cybersecurity related privacy events
	Reference	https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf
	SENTINEL dimension	Data privacy
Other benchmarks		
SparkBench	Type	Benchmarking suite
	Description	SparkBench comprises four main workload categories: machine learning, graph processing, streaming, and SQL. The objective is to optimise the clusters and analyse trade-offs between different designs in SPARK-based systems.
	Metrics	Job execution time, data process rate.
	Reference	https://codait.github.io/spark-bench/
	SENTINEL dimension	Architecture, data management (especially since some of the implementation in SENTINEL use SPARK, e.g., Data Fusion Bus)
GDPRbench	Type	GDPR benchmark
	Description	GDPRbench is an open-source benchmark designed specifically to assess the GDPR compliance of database systems which means how well a storage solution responds to common GDPR queries. The benchmark provides workloads and metrics to understand and assess personal-data processing database systems by providing

		quantifiable measurements concerning the correctness and performance of databases under GDPR.
	Metrics	Correctness against GDPR workloads, time taken to respond to GDPR queries, and storage space overhead.
	Reference	https://www.gdprbench.org https://github.com/GDPRbench/
	SENTINEL dimension	Privacy, compliance
Autonomous Digital Enterprise (ADE) Index	Type	Digital Competitiveness benchmarking tool
	Description	ADE Index assesses organisational maturity across technology-enabled tenets.
	Metrics	Adaptive Cybersecurity
	Reference	https://www.bmc.com/corporate/autonomous-digital-enterprise.html?vu=ade
	SENTINEL dimension	Innovation
The OECD Privacy framework	Type	Framework
	Description	OECD Privacy Guidelines - The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data constitute the first update of the original 1980 version that served as the first internationally agreed upon set of privacy principles. Two themes run through the updated Guidelines: • A focus on the practical implementation of privacy protection through an approach grounded in risk management, and The need to address the global dimension of privacy through improved interoperability.
	Metrics	
	Reference	https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
	SENTINEL dimension	Data privacy, data protection compliance
MetricStream	Type	Software as a Service
	Description	It is a Governance, Risk Management, and Compliance (GRC) platform supplying a technology infrastructure for deploying GRC apps configurable to meet the needs of the enterprise.
	Metrics	Governance, Risk & Compliance such as: • Common repository of GRC items • Risk management • GRC policy management Incident management
	Reference	https://www.metricstream.com
	SENTINEL dimension	Data protection compliance
Servicenow	Type	Software as a Service
	Description	The solution helps business users ensure compliance to regulations, policies, standards and frameworks. It is available via the Standard, Professional, and Enterprise editions, the latter two supporting GRC and internal auditing processes
	Metrics	GDPR
	Reference	https://www.servicenow.com
	SENTINEL dimension	Data protection assessment tools & services
Archer	Type	Software as a Service

	Description	RSA Archer, from the security, governance, and risk division of RSA Security is an integrated risk management / GRC platform.
	Metrics	----
	Reference	https://www.archerirm.com/
	SENTINEL dimension	GDPR compliance
OneTrust Pro	Type	Software as a Service
	Description	OneTrust offers growing businesses powerful and easy-to-use privacy and security compliance tools that provide one place for privacy, security, marketing, and third-party risk managers to work together.
	Metrics	Data Governance, Governance, Risk & Compliance, Vendor Risk Management, Data Privacy Management
	Reference	https://www.onetrustpro.com
	SENTINEL dimension	Data protection assessment tools & services
TrustArc (Planner & Benchmarks)	Type	Software as a service
	Description	Planner & Benchmarks assists the privacy office in building, documenting, and maintaining a structured privacy program. Enabled organizations baseline the status of their program – empowering privacy leaders to compare their progress with other organizations based on their size, region, or industry. As a trusted partner to the business, quickly identify program blockers and gaps and make data driven decisions that mitigate privacy risk and deliver impactful accountability
	Metrics	GDPR, CCPA & LGPD Alignment
	Reference	https://trustarc.com
	SENTINEL dimension	Data protection assessment tools & services
	Comments	A single platform experience delivered through a combination of privacy frameworks, insights, intelligence, knowledge and operations. Its data inventory and mapping capabilities allow users to create an inventory of IT systems, third parties (vendors) and company affiliates relevant to data flows and potential risks across an organization. Its PrivacyCentral privacy management component is a data intelligence centre and workflow tool that aims to help users reduce inefficiencies and stop the endless cycle of regulation dependency.

2.4.2 User centric benchmarks and standards

Abiding by mandate of the SENTINEL project the following user centric benchmarks and standards might be applicable:

- **eGovernment Benchmark Framework**[3] the benchmark analysis takes place along the lines of four top-level benchmarks:
  - User-centric Government
  - Transparent Government
  - Cross Border Mobility

[3] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=55174

  - Key enablers

- **Web Content Accessibility Guidelines (WCAG 2.1)**[4] is an extension of WCAG 2.0. It considers the new and different ways we use existing technology, factors in new forms of technology and includes new criteria that looks at users with low vision and cognitive abilities, while still making sure that digital content remains accessible. WCAG remains the benchmark standard in assessing the accessibility of a website.
- **ISO 9241-210:2019**[5] **Ergonomics of human-system interaction**. **Part 210: Human-centred design for interactive systems**”. The ISO 9241 is a multi-part standard from the International Organization for Standardization (ISO) covering ergonomics of human-computer interaction. It is managed by the ISO Technical Committee 159. Part 210 provides requirements and recommendations for human-centred design principles and activities throughout the life cycle of computer-based interactive systems. In addition, **ISO 9241 Part 110 and ISO 9241 Parts 11–19** deal with usability aspects of software, including a general set of usability heuristics for the design of different types of dialogue (ISO 9241-110:2020[6]) and general guidance on the specification and measurement of usability (ISO 9241-11:2018[7]).

2.4.3 Business privacy benchmarks

An important aspect of assessing the impact of CS and PDP technologies in SMEs is by comparing the achieved business benefits with those of their peers. In this way they can revise their choices or their organization if they find they are achieving less results than median benchmarks for their business sector and company size.

Benchmarks such as (Deloitte, 2018; CISCO, 2021; TrustArc, 2021) are based on studies exploring the practices and maturity levels at organisations around the world, focusing on aspects such as financial investments in CS and PDP, business benefits from these investments, time to compliance with new privacy regulations, etc.

Using business benchmarks, we can compare the experimental results obtained in SENTINEL with those obtained in the context of similar business cases. Special attention will be provided in the context of SENTINEL experimentation to identify further benchmarks that are applicable to SMEs.

[4] https://www.w3.org/WAI/standards-guidelines/wcag/glance/
[5] https://www.iso.org/standard/77520.html
[6] https://www.iso.org/obp/ui/#iso:std:iso:9241:-110:ed-2:v1:en
[7] https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en

3 Contextualising the experimentation process

The experimentation process described in Section 2, will be grounded in a number of real-life cases to be carried out in WP6. These will concern three pilots namely those of ClinGenics (CG), Tristone Investment Group (TIG) and SMEs engaged via the UNINOVA Digital Innovation Hub and incubator.

This Section describes the business cases and challenges for the three pilot cases which in turn provide the backdrop to the validation variables in Section 5.

3.1 Pilot 1: ClinGenics

ClinGenics (UK) Ltd (CG) is a UK company founded in late 2016, with the aim of advancing patient care and support through the development and provision of state-of-the art decision-support and cutting-edge solutions in Genomic Medicine for physicians and patients.

The final variant interpretation report provided by CG has the added important feature of incorporating expert manual curation, personalized interpretation and case-specific comments and suggestions for further actions, thus fulfilling its role as a true decision support tool.

Case overview	To ensure security and privacy of genomic and of user/client data.
Case company	ClinGenics Ltd.
Business context	CG's provides decision-support solutions to address the complexities associated with genomic variant interpretation and the clinical interpretation of DNA variants associated with genetic diseases, aiding the diagnosis of hundreds of complex and rare disorders.
Provided solution	The Exome Management Application (EMA), which is a bioinformatics platform-software pipeline, coupled to expert curation for the evaluation and reporting of actionable genomic variants.
Current capabilities	The EMA pipeline software currently provides a number of types of variant data interpretation services. For large scale projects or other research applications, a dedicated custom variant analysis is also available upon request, for generating population-specific common variant database(s). The results are made available as a database in SQL file format or custom report may be generated.
The SENTINEL challenges	To ensure: (a) privacy of identifiable information (PII) during the submission process (b) security protection of all stored data, etc. and (c) the limitation of any type of unauthorized access to the data.

3.2 Pilot 2: Tristone Investment Group

Tristone Investment Group (TIG) is an independent investment company committed to the acquisition and growth of established, social care organisations that deliver positive social impact. Specifically, TIG is focused upon delivering exemplary standards of care, support and education to children, young people, and vulnerable adults. TIG has been founded upon the principles of Ethical Capitalism being passionate about the notion that sustainable commercial success can, and should, align with positive social impact.

All businesses within the group have a high degree of autonomy, covering a range of services and specialisms, all of which operate within specific conditions of important legislative and regulatory frameworks, as well as established models of service delivery. In the context of SNETINEL experiments we will focus one of these businesses, namely that of JUVENTAS.

Case overview	**To ensure quality social care services and safeguard vulnerable people.**
Case company	JUVENTAS SERVICES LTD.
Business context	JUVENTAS is a care provider that provides the following services: supported accommodation for young people (16-25 years); supported accommodation to Unaccompanied Asylum-Seeking Children (UASC); residential children's homes.
Provided solution	To do this effectively, JUVENTAS collects, processes and stores information about service users that is highly-sensitive. Depending upon the circumstances, the above information must be shared with designated employees (only) of commissioning authorities, regulators (sector specific) and auditors.
Current capabilities	The flow of information is administered from administrational centres and individual settings. It is the responsibility of each respective manager to ensure that relevant and lawful data protection principles are maintained. The systems and processes we use to manage data are broad and subject to clearly defined principles of conduct. The conduct of colleagues is defined through policy and augmented through induction processes, confidentiality agreements, training, supervision and managerial oversight.
The SENTINEL challenges	To ensure: (a) governance and compliance with regulation and high standards of practice; (b) robust and effective risk management processes; (c) outcomes monitoring, analysis and accountability.

3.3 Pilot 3: SMEs/MEs engaged via UNINOVA[8]

The SENTINEL's third pilot is based on a digital innovation hub (DIH- inNOVA4TECH) and a relevant incubator / accelerator (Madan Parque) provided through UNINOVA.

The inNOVA4TECH DIH operates in a pan-European level and is located in Portugal. Its customers include start-up companies, SMEs (<250 employees), MidCaps (between €2-10 billion turnover), Large companies, multi-nationals, as well as research organisations. Among other, the DIH services are targeting the research, technology, and health services, being the DIH fully aligned with the RIS3 strategy.

The potential of inNOVA4TECH ecosystem can also be leveraged through the partnerships with Madan Park and AISET, which accounts for more than 200 associate companies, more than 10 regional and national associations, and more than 10 thematic networks.

Most of the aforementioned services include challenges related to data privacy and protection as well as specific needs for compliance with relevant regulations. In the following, some indicative specific cases are summarized with respect to the specific challenges.

[8] UNINOVA Digital Innovation Hubs and incubators

Case overview	**Application Digitization of a Back Pain and Musculoskeletal Disease Machine to Support the Patient Monitor**
Case company	Physiotherapy centres
Business context	Digitalize the physiotherapy machine for recovery of back pain, in order to accompany the patient during the exercise and in this way give indications if the exercise is being done correctly.
Provided solution	Sensors are being implemented in the machine to be able to remove the patient's exercise monitoring, so that a digital twin of the machine can be produced, and to identify whether the patient is performing the exercise correctly, taking into account the patient's ethics.
Current capabilities	Cyber-Physical Systems; Internet of Things; Artificial Intelligence and cognitive systems; Interaction Technologies (human-machine interaction); Augmented and virtual reality, visualization; Internet services, Digital solutions for government
The SENTINEL challenges	To ensure that all sensitive data related to these physiotherapy centres are handled in a secure and trustworthy manner, based on specific regulatory frameworks and facilitated by the necessary data privacy services.

Case overview	**Application to monitor the safety and well-being of shop floor workers**
Case company	PRODUTECH
Business context	It is intended to support factories to improve hygiene and safety at work, through the implantation of devices and application development, considering ethics at work.
Provided solution	It is intended to introduce devices in the factories to monitor the operator in operations that bring occupational diseases, to support reduce or prolong the appearance of this disease. At the same time, it is intended to develop applications that support increase safety at work by notifying operators about the safety distance to avoid contagion of the COVID-19, another solution to be developed is an application to measure the temperature of operators whenever they enter the factory. To be done automatically and avoid exposure by another operator.
Current capabilities	Cyber-Physical Systems; Internet of Things; Artificial Intelligence and cognitive systems; Augmented and virtual reality, visualization; Internet services
The SENTINEL challenges	Analyse potential data breaches with respect to sensitive personal data; identify regulations related to workers' monitoring and diseases' reporting and provide the related compliance and data protection services.

Case overview	**Application to control the polishing process to optimize cutlery production.**
Case company	CRISTEMA

Business context	CRISTEMA is a cutlery production company, it aims to solve a bottleneck problem that happens in the cutlery polishing phase, which is made by one machine, producing a delay in the factory production. It aims to optimize and improve the cutlery production process.
Provided solution	Sensors were placed on the polishing machine in order to count the pieces and be able to identify what was being produced, followed by an application that contains weekly production orders and automatically generate weekly planning for the polishing process, taking into account the type of cutlery, quantity and quality. In this way it was possible to count the cutlery that was being polished and check if the planning deadlines are being fulfilled.
Current capabilities	Cyber-Physical Systems; Internet of Things; Artificial Intelligence and cognitive systems; Augmented and virtual reality, visualization; Simulation and modelling; ICT management, logistics and business systems.
The SENTINEL challenges	To identify potential Industrial IoT-related data sets that are sensitive for the core business of CRISTEMA; analyse potential regulatory frameworks related to Industrial IoT data management; and provide the required data privacy and compliance mechanisms.

4 Verification variables for the SENTINEL digital framework

This Section describes the verification templates that will be used for each technology component of the SENTINEL platform. At this stage the focus is on determining the appropriate quality variables. Where possible associated metrics, baseline values and associated technology benchmarks are also indicated. However, these aspects will be further elaborated and refined in later phases of the experimentation process.

4.1 The SENTINEL digital platform assets

Figure 2 provides an overview of the current version of the architecture of the SENTINEL digital platform. The value of Figure 2, in the context of this deliverable, is its clear identification of the SENTINEL platform components, thus providing a clear path to identifying appropriate verification variables related to each one of these components as well as to the overall integrated system.

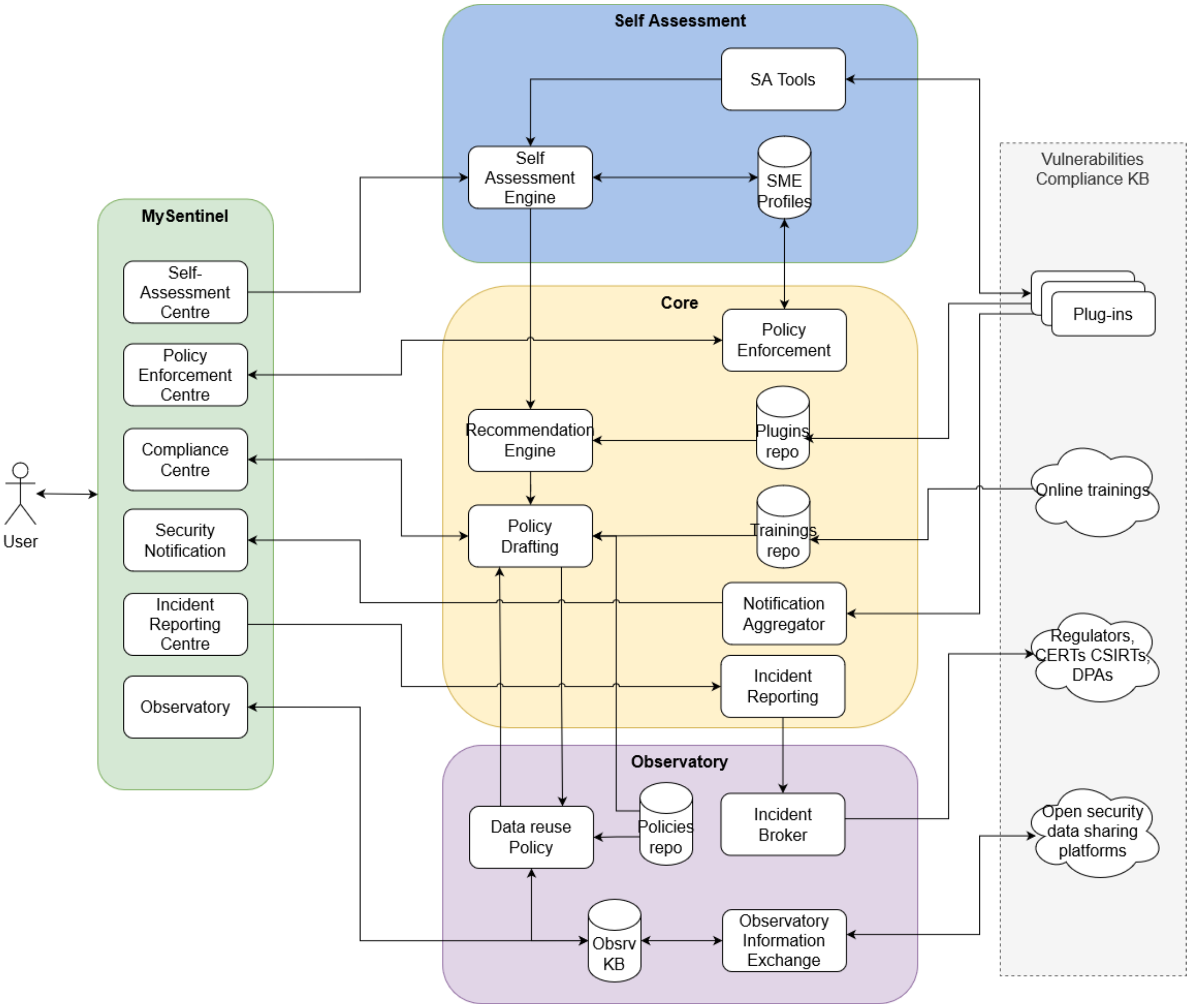

Figure 2. The SENTINEL architecture

As shown in Figure 2, the integrated platform consists of four (4) core components (called ***contexts***), namely: *MySentinel*, *Self-assessment*, *Core* and *Observatory*. Each context is a collection of modules (software systems) that operate under a common setting. For example, MySentinel represents a grouping of front-end modules, all of which aggregate data to SENTINEL's primary dashboard. In addition, to these core components a number of optional software components (referred to as ***plugins***) can be optionally integrated into the SENTINEL platform, providing additional capabilities. These include (not detailed in the diagram): *Security Infusion*, *IdMS*, *GDPR self-assessment*, *MITIGATE*, *SPAP*, *Cyber Range*, *Forensics Visualisation Toolkit*, as well as other external plugins. For a detailed description of the architecture please refer to deliverable D1.2 "The SENTINEL technical architecture".

As mentioned in Section 2.3.1, verification aims to evaluate the quality of the SENTINEL digital platform in parts and as a whole. Therefore, the object of verification experiments can be a specific SENTINEL *plugin*, a *context* of the SENTINEL digital platform framework, or the *integrated* SENTINEL *platform*. To this end, the following Sections 4.2 and 4.3 identify the verification variables and associated metrics for each plugin and core component of the SENTINEL architecture. It should be noted that this is an initial list that will be further detailed and finalised during the experimental alignment phase in WP6.

4.2 Verification variables of SENTINEL plugins

Asset	Verification variable	Metric	Baseline Value	Benchmark	Expected result	Relevant KRs
Security Infusion (ITML)	Security	no. of threats and system vulnerabilities detected accuracy of detection	N/A			KR-3.1 KR-3.2
	Data integrity	accuracy of data modification detection	N/A			KR-3.2
IdMS (The Shell)	Transparency	ease of access to view and manage data				KR-3.1 KR-2.5
	Functional suitability / Verify implementation of GDPR user rights (access, information, rectification, erasure, portability, etc.)	Boolean	False	GDPR	True	KR-3.2
	Confidentiality (data encryption at rest and in transit)	Boolean	False		True	KR-3.2 KR-2.4 KR-2.5
	Authentication and authorization (verify implementation	Boolean	False		True	KR-2.4

	of SSO mechanism)					
	Usability	task completion time / clicks, user's subjective satisfaction				KR-1.4
GDPR self-assessment (LIST)	Functional suitability / Verify appropriateness of measures implemented to comply with GDPR	Boolean	False	GDPR	True	KR-3.1 KR-3.2
	Functional suitability / Verify effectiveness of measures implemented to comply with GDPR	Boolean	False	GDPR	True	KR-3.2
	Functional suitability / Identify areas for improvement of measures appropriateness and effectiveness	Boolean	False	GDPR	True	KR-3.2
	Usability / Learnability / Identify how to improve compliance with GDPR	Boolean	False	N/A	True	KR-3.2
MITIGATE - Risk Management Component (FP)	Security	no. of assets registered	N/A			KR-3.1 KR-3.2
	Security	no. of threats registered	N/A			KR-3.2
	Security	no. of vulnerabilities detected for registered Assets	N/A			KR-3.2
	Security	no. of risks calculated	N/A			KR-3.2
	Data integrity	accuracy of data modification detection	N/A			KR-3.2
	Response time	measured time occurred between request to and response from Risk Management Component	Single node, baseline Risk Management			KR-3.4

			Component response time			
Security and Privacy Assurance Platform (STS)	Ability to assess GDPR/custom defined compliance organizational measures	Boolean	N/A			KR-3.1 KR-3.2
	Ability to assess GDPR/custom defined compliance technical measures	Boolean	N/A			KR-3.2
	Ability to assess technical measures effectiveness	Boolean	N/A			KR-3.2
	Maintenance of accountability records for personal data access	Boolean	N/A			KR-3.2
CyberRange (ACS)	Ease of integration	setup overhead				KR-1.1 KR-3.1
	Security	no. of infrastructure assets supported	N/A			KR-3.2
	Security	no. of vulnerabilities detected	N/A			KR-3.2
Forensics Visualisation Toolkit (AEGIS)	Usability	task completion time / clicks, user's subjective satisfaction				KR-1.4 KR-3.1
	Performance	page load time, response time				KR-3.4
	Effectiveness	no. of data-driven dashboard widgets supported perceived relevance of data				KR-3.4 KR-4.5
Open source and external plugins (TSI)	Functional suitability	no. of requirements achieved	N/A			KR-3.1, KR-3.2
	Ease of integration	setup overhead				KR-1.1
	Maintainability	support community size				KR-1.1

4.3 Verification variables of core SENTINEL components

Asset	Verification variable	Metric	Baseline value	Benchmark	Expected result	Relevant KRs
MySentinel (AEGIS)	Usability	task completion time / clicks, user's subjective satisfaction				KR-1.4
	Accessibility	colour contrast, alt text for images		WCAG 2.1		KR-1.4
	Performance	page load time, response time				KR-3.4
	Privacy (compliance to privacy laws)	user-sensitive data protection regulations		GDPR		KR-3.2
	Availability	percentage of requests satisfied				KR-3.4
Self-assessment (IDIR)	Extensibility (adding features, and carry-forward of customizations at next major version upgrade)	ability to easily incorporate new self-assessment capabilities				KR-2.1
	Availability	percentage of requests satisfied				KR-3.4
Core (ITML)	Performance	average response time to requests accuracy of recommendations				KR-2.2 KR-3.4
	Scalability (horizontal, vertical)	throughput increase per node added resource usage drop per node added				KR-3.3
	Availability	percentage of requests satisfied				KR-3.4
Observatory (ITML)	Interoperability	no. of data exchange interfaces implemented				KR-4.5
	Availability	percentage of requests satisfied				KR-3.4
Integrated platform (INTRA)	Functional suitability	pass end-to-end tests for all usage scenarios (pass/fail)				KR-1.1 KR-2.3 KR-3.1 KR-3.2 KR-4.2

The three columns of Baseline value, Benchmark and Expected result, will be completed during the planning phase in task T6.1.

5 Validation variables for the SENTINEL pilot experiments

According to the GA, SENTINEL will carry out five (5) demonstrators in different SMEs industries and environments (KR-4.3). In doing so it will collect data for demonstrating automated data privacy and protection compliance procedures (KR-4.1). SENTINEL operational experiments will be defined on the basis of the real pilot cases within the business sectors where the project's SME partners are involved (reported in Section 3). In addition, complementary experiments may be defined in the same use case. The following experiments are only indicative at this point. Their definition will be further elaborated in the context of WP6. Using these pilot experiments the project will carry out a minimum of ten (10) trials to demonstrate the applicability of the SENTINEL tools (KR-4.4).

5.1 CG pilot experiments overview

CG pilot aims to test the efficiency of the SENTINEL platform in the context of: (a) proactively implementing stringent security layers regarding the access and use of genomic data as well as (b) ensuring privacy and security of client/user data. To this end, the following two operational experiments have been defined, as shown in Table 9 and Table 10.

Table 9. CG 1st experiment definition

Experiment name	**Security of user/client data**	
Experiment's Goal(s)	To test the efficiency of SENTINEL in ensuring user/client data privacy without negatively affecting CG productivity.	
Experiment's Variables	Service quality, User satisfaction, Efficiency, Compliance, Threat containment	
Experiment Workflow	Stage One: Set Up Stage two: Implementation *These will be defined in detail during the planning phase.*	
Participants	Role	Number of Individuals
	CG Administrator	1
	CG Expert Staff	1

Table 10. CG 2nd experiment definition

Experiment name	**Proactive security of genomic data**
Experiment's Goal(s)	To test the efficiency of SENTINEL in improving privacy and secure access of genomic data without negatively affecting CG productivity.
Experiment's Variables	Service quality, User satisfaction, Efficiency, Compliance, Threat containment

Experiment Workflow	Stage One: Set Up Stage two: Implementation *These will be defined in detail during the planning phase.*	
Participants	Role	Number of Individuals
	CG Administrator	1
	CG Expert Staff	1

The validation variables and associated metrics towards which the measurement will be performed in both experiments are summarised in Table 11.

Table 11. CG experiments validation variables

	Validation variable	Metric	Baseline value	Benchmark	Expected result	Actual result	Relevant KRs
Business	Service quality	Time to submit case-related clinical information					
	User satisfaction	End user experience survey					KR-1.4
	Efficiency	% increase in privacy awareness % decrease in productivity					KR-1.4
CS & PDP	Compliance	No of Anosymisation and pseudonymisation techniques implemented Patient-specific identifiers detected					KR-1.2
	Threat containment	Security risks detected Security risks mitigated					KR-1.5
	Data breach prevention	No of incidents detected No of incidents prevented					KR-1.5

5.2 TIG pilot experiment

TIG pilot experiment aims to assess the efficiency of the SENTINEL platform in assisting TIG Juventas to provide safe and reliable care services, as summarised in the following Table 12.

Table 12. TIG Juventas experiment overview

Experiment name	**TIG Juventas pilot case**	
Experiment's Goals	To test the efficiency and effectiveness of the SENTINEL framework in the context of TIG Juventas Services provisions.	
Experiment's variables	Customer satisfaction, service user safety and compliance	
Experiment Workflow	Stage One: Set Up Stage two: Implementation *These will be defined in detail during the planning phase.*	
Participants		
STAGE ONE: Set Up	Role	Number of Individuals
	Company Administrator	1
	Service Manager	1
	DH (TIG)	1
STAGE TWO: Implementation	Role	Number of Individuals
	Company Administrator	1
	Service Manager	1
	Staff (TBC)	2
	DPO	1
	DH (TIG)	1

Table 13 shows the validation variables and associated metrics to be used in this experiment.

Table 13. TIG Juventas experiment's validation variables

	Validation variable	**Metric**	**Baseline value**	**Benchmark**	**Expected result**	**Actual result**	**Relevant KRs**
Business	Service user satisfaction	Time to provide service	No of days to provide user service		Decrease 5%		
	Cost efficiency	Price of technologies	Price of existing solution, based upon cost of manual administration of existing structure. Time spent against time saved		50% reduction of cost		KR-1.3
s	End-user satisfaction	User response (1-5 scale)	4		5		KR-1.4
CS & PDP	Service User Data Privacy	No of incidents / month	0 - No incidents reported in Juventas since 30/10/20. This must be maintained		No increase		KR-1.5
		No of threats avoided	N/A		5		

	Validation variable	Metric	Baseline value	Benchmark	Expected result	Actual result	Relevant KRs
	Compliance	% of compliance standard used	Standards used		100% compliance		KR-1.2

5.3 Generic Experiment

Generic experiments aim to demonstrate the general applicability and usability of the SENTINEL platform from the perspective of potential generic end-users such as the customers of DIH-inNOVA4TECH. In this way, the SENTINEL offerings will be communicated through Digital Innovation Hubs (KR-5.4). The overview and validation variables of the generic experiment are presented in Table 14 and Table 15 respectively.

Table 14. Generic experiment overview

Experiment name	Generic experiment	
Experiment's Goal(s)	To evaluate user experience of SENTINEL in different contexts	
Experiment's Variables	Satisfaction, Performance, Service quality, Time efficiency, Cost/effort reduction, Customer satisfaction, Uptime, Compliance, Threat containment, Data breach prevention	
Experiment Workflow	Stage One: Set Up Stage two: Implementation *These will be defined in detail during the planning phase.*	
Participants	**Role**	**Number of Individuals**
	Business Administrator	1
	Staff	1
	DPO (if applicable)	1
	IT Information Security officer	1

Table 15. Generic experiment's validation variables

	Validation variable	Metric	Baseline value	Benchmark	Expected result	Evaluators	Relevant KRs
Business	Satisfaction	User score on scale 1-5					KR-1.4
	Performance	Resource utilization					KR-1.4

	Validation variable	Metric	Baseline value	Benchmark	Expected result	Evaluators	Relevant KRs
	Service quality	Evaluator's score on scale 1-5 Innovative features compared to existing cybersecurity and privacy management solutions					KR-1.4
	Customer satisfaction	No of complaints Increased customer trust					KR-1.4
	Cost/effort reduction	Cost effectiveness compared to other cybersecurity and privacy management solutions CS and PDP investment ROI					KR-1.3
	Time efficiency	Average response time to customer request Privacy Impact Assessment (PIA) completion rate					KR-1.4
CS & PDP	Uptime	Time to incident detection					KR-1.4

	Validation variable	Metric	Baseline value	Benchmark	Expected result	Evaluators	Relevant KRs
		Time to incident resolution Incident workload					
	Compliance	Results of privacy internal audits Increased awareness of regulatory frameworks	1.Comprehensive and updated Data Protection Policy in place 2.Informed consent procedures applied (incl. information notices, consent forms, procedures for the exercise of data subject's rights) 3.Appropriate organizational/security measures in place, equivalent to the ISO/IEC 27001:2013 standards 4.Appropriate protocols enacted on data minimization, including anonymization				KR-1.2

	Validation variable	Metric	Baseline value	Benchmark	Expected result	Evaluators	Relevant KRs
			techniques				
	Threat containment	Security risks detected Security risks mitigated					KR-1.5
	Data breach prevention	No of incidents detected No of incidents prevented No of incidents resolved					KR-1.5

6 Reflection of the experimentation variables on SENTINEL Key Results

Assessing the project's impact is done through KRs and their related measurable KPIs. The KRs and KPIs as defined in the GA are presented in Appendices A and B respectively. These will be continuously monitored and if necessary or desirable they will be revised according to emergent project results.

A key evaluation aspect during the experimentation process is the degree of achievement of project objectives. The focus of this evaluation is on the KRs. As shown in preceding sections, we have carried out an analysis of the way that verification and validation are related to KRs and included the correspondence between the experimentation variables and KRs in the relevant tables. The value of including this correspondence in the verification and validation templates, is significant in acting as a monitoring tool and a guide during the experimentation process.

KRs are examined through the KPIs defined by the consortium. They are considered an indispensable management tool of the project that will allow us to monitor the progress, enable evidence-based decision-making, and aid in the development of strategies.

The SENTINEL Consortium has defined KPIs organised into three categories, namely Research and Innovation (R&I) KPIs, Business KPIs and Dissemination KPIs. The R&I KPIs will be continuously monitored by the Project Coordinator (ITML) and the Scientific Technical and Innovation Manager (INTRA). The Business KPIs will be monitored by the Quality Assurance Manager (ITML) and Dissemination KPIs will be monitored by the Dissemination and Exploitation Manager (UNINOVA).

One of the objectives of task T1.3 (see Section 1.1) has been to review KRs and KPIs in light of the work done thus far in the project. Significant progress has been made so far in technical areas, such as the refinement of the SENTINEL architecture, as well as in user-facing needs and expectation of SME stakeholders from their involvement in the pilot cases as well as in the value they expect to get from the SENTINEL offerings beyond the experimentation stage.

At this stage, and because of the aforementioned progress in the project, we are in a position to offer some insights as to the need for potential revisions to KRs and KPIs, revisions that seek to clarify a number of them, to make their values more quantitative and to remove any uncertainty as to their description. To this end, we present in Table 16 these insights.

Table 16. Suggested KR/KPI revisions

KPI or KR	Existing description	Suggested revised description	Existing value	Suggested revised value	Rationale
Technology KRs					
KR-1.2	40% improved compliance efficiency for SMEs/MEs	40% efficiency boost in achieving and demonstrating evidence based GDPR compliance for SMEs	unchanged		For detail, clarity and legibility in the KR description

KR-1.5	Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility	Offer tangible solutions to SMEs, addressing all six (6) STRIDE threat model-based security threat categories	10	6	For a technically precise and fit-for-purpose KR description
KR-2.2	Accuracy of (distributed) machine (deep) learning algorithms facilitating intelligence in the recommendations for data compliance of more than 80%	At least 80% accuracy of AI/ML-based recommendation technologies for cybersecurity and personal data protection	unchanged		For detail, clarity and legibility in the KR description
KR-2.3	Test data privacy compliance engine in terms of speed and accuracy	Offer a comprehensive and usable digitalised DPIA and GDPR compliance self-assessment framework	N/A		Proposing a more fit-for-purpose KR description, aligned with the refined technical architecture
KR-2.4	Accuracy of data access management and authentication mechanisms offered to SMEs/MEs more than 90%	Offer robust and easy to adopt authentication, authorisation and record keeping technologies to SMEs for GDPR compliance	90%	N/A	KR description better aligned with the refined technical architecture
KR-3.1	More than (20) novel services and tools utilised and integrated from diverse multi-domain technological areas and applied in SMEs/MEs environments	At least twenty (20) novel cybersecurity and personal data protection technologies and tools offered to and applied by SMEs	unchanged		KR description for clarity, legibility and alignment with the refined technical architecture
KR-3.2	At least (10) tools and services related to data protection, data privacy management, security assurance and compliance	At least ten (10) novel technologies and tools offered to and applied by SMEs, directly addressing PDP awareness and GDPR compliance needs	unchanged		For detail, clarity and legibility in the KR description
KR-3.4	Accuracy and efficiency of the SENTINEL data privacy compliance recommendation engine at least 70%	At least 70% accuracy of AI/ML-based recommendation technologies for GDPR compliance	unchanged		For detail, clarity and legibility in the KR description
Validation / impact KRs					
KR-4.1	Successful collection of data for demonstrating automated data privacy and protection compliance procedures in complementary SMEs/MEs environments	Successful collection and leveraging of data for recommending personal data protection technologies and GDPR compliance procedures in complementary SME environments	N/A		For detail, clarity and legibility in the KR description
KR-4.5	Construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs	Offer efficient and intuitive data-driven assessments and visualisations for SME cyber awareness and decision support	N/A		KR description for clarity, legibility and alignment with the refined technical architecture

KR-5.2	Uptake more than (6) standards from several data privacy and compliance related technologies	Uptake of at least six (6) standards, regulations and guidelines for personal data protection-related compliance.	unchanged		For additional clarity in the KR description
KR-6.1	Ready to market integrated solution for the overall security compliance framework and independent data privacy and security enhancing solutions (TRL 7)	Offer a market ready (TRL 7) integrated solution for cybersecurity and personal data protection, tailored to SMEs	TRL 7		Improved KR description
KR-6.2	At least four (4) SENTINEL tools reach market readiness level eight (8) at the end of the project	At least four (4) SENTINEL tools reaching market readiness level eight (8) at the end of the project as advocated in relevant literature(S.S. Solberg Hjorth and Brem, 2016; cyberwatching.eu Consortium, 2018)	unchanged		Improved KR description
KR-6.3	At least six (6) third party collaborations to be established for further applicability verification	At least six (6) third party collaborations to be established for further verification	unchanged		Improved KR description
Impact / business KPIs					
iKPI2.2	Number of Digital Innovation Hubs engaged by the end of the project		Over 8	At least 5	Setting a better-informed target value following initial work
iKPI4.3	Number of stakeholders and third parties engaged	Number of entities and third parties reached	10.000 smaller enterprises from at least 6 countries	10 000 SME stake-holders from at least 6 countries	For clarity. This KPI refers to digital dissemination and awareness campaigns results (i.e., email and PPC marketing)
iKPI10	Number of cases testing and validating the innovative capacity of the SENTINEL's offerings	Number of cases testing and validating the innovative capacity of the SENTINEL offerings	>5	≥5	Improved syntax & setting a more informed target value following initial work
iKPI11.1	Number of third-party entities (SMEs/MEs) directly using SENTINEL's tools/services		>20	>25	Setting a more informed target value following initial work
iKPI12.1	iKPI12.1: Number of start-ups and spin-offs boosted exploiting SENTINEL security services		>4	>6	Setting a more informed target value following initial work

iKPI13	Increase in sales for the pilot partners exploiting SENTINEL platform	Increase in cyber resilience for pilot partners fully adopting SENTINEL	>15%	>45%	Better-worded KPI, setting a more informed target value following initial work

7 Conclusions

Deliverable D1.3 is the result of the work that was carried out in task T1.3. It should be noted that this work has been informed by the two other tasks within Work Package WP1, namely those of T1.1 and T1.2. The former established the baseline for SENTINEL and it has been especially relevant to T1.3 in terms of the challenges and needs of SMEs for CS and PDP. The latter has set a clear view for the development of the SENTINEL architecture which set the backdrop for the establishment of verification and validation variables considered by T1.3 and reported in this deliverable.

This deliverable provides details about the process of experimentation, as well as providing a detailed definition of the variables to be used during experimentation for the purposes of verification and validation. These variables are juxtaposed against benchmarks and standards in order to ensure a high degree of objectivity when the experimental results are analysed.

To ensure uniformity across all aspects of experimentation this deliverable puts forward two templates, that were used by SENTINEL stakeholders (technologists and users) to define those variables and metrics that are deemed relevant for evaluating their contributions in the project.

The experimentation protocol discussed herein will, according to the GA, be finalised in Work Package WP6, based on more detailed user requirements. It should be noted that such requirements have already been captured and to a large extent analysed and reported in deliverable D1.1. However, within WP6 the experimentation protocol will become more closely aligned to the environments of SMEs including the selection of respective industrial sub-systems and hardware components for demonstration purposes and utilisation of simulation(s) in case critical parts of the infrastructure are needed. The execution of the trials, using the experimentation protocol presented in this report, is expected to be an iterative process starting with early versions of the SENTINEL solution (M12 and M18) that may have limited functionality, and moving to more in-depth experimentation as more functionality is added.

Acknowledgments

We wish to thank our technology colleagues in the SENTINEL project for their contributions to completing the verification template presented in Section 4 and to SME colleagues for their contributions to completing the validation template in Section 5. More generally we are grateful for the valuable discussion during technical meetings with colleagues across the SENTINEL consortium. We would like to express our gratitude to our internal project quality reviewers for their valuable contribution to ensuring the high quality of this deliverable.

IDIR: Evangelia Kavakli, Pericles Loucopoulos, Yannis Skourtis

8 References

Basili, V. R. & Rombach, D. D. (1988). *The TAME Project: Towards Improvement-Oriented Software Environments*. IEEE Transactions on Software Engineering*,* Vol. 14**,** No. 6, pp. 758-773.

Brusa, E., Calà, A. & Ferretto, D. (2018). *Systems Engineering and Its Application to Industrial Product Development*, Springer.

CISCO (2021). *Data Privacy Benchmark Study: Forged by the Pandemic -The Age of Privacy*. CISCO Secure.

CWA (2010). *CWA 16113:2010 Personal Data Protection Good Practices*. European Committee for Standardisation.

cyberwatching.eu Consortium (2018). *Methodology for the Classification of Projects/ Services and Market Readiness*. The European watch on cybersecurity & privacy.

DataBench Consortium (2019). *Deliverable D1.1 - Industry Requirements with benchmark metrics and KPIs*.

Deloitte (2018). *The Deloitte General Data Protection Regulation Benchmarking Survey*. Deloitte.

ENISA (2015a). *Cloud Security Guide for SMEs: Cloud computing security risks and opportunities for SMEs*. European Union Agency for Network and Information Security.

ENISA (2015b). *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*. European Union Agency for Network and Information Security.

ENISA (2016). *Guidelines for SMEs on the security of personal data processing*. European Union Agency for Network and Information Security.

Fotrousi, F., Fricker, S. A., Fiedler, M. & Le-Gall, F. (2014). *KPIs for Software Ecosystems: A Systematic Mapping Study*. *In:* Lassenius, C. & Smolander, K. (eds.) "ICSOB 2014"*.* Springer International Publishing.

Hewitt, K. (2021). *Key Performance Indicators (KPIs) for Security Operations and Incident Response. Identifying Which KPIs Should Be Set, Monitored and Measured.*

ISO/IEC (2011a). *Information technology — Security techniques — Privacy framework*. Technical Committee: ISO/IEC JTC 1/SC 27 ICS : 35.030 IT Security, International Standards Organisation.

ISO/IEC (2011b). *Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models*. ISO/IEC 25010:2011(E), ISO/IEC.

ISO/IEC (2013). *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC 27001:2013, International Standards Organisation.

ISO/IEC/IEEE (2015). *Systems and software engineering — System life cycle processes*. International Standards Organisation.

Jaquith, A. (2007). *CHAPTER 3 Measuring Security Program Performance*. "Security Metrics, Replacing Fear, Uncertainty, and Doubt"*.* Addison Wesley. pp. 117-196.

Ponemon Institute (2010). *Security Effectiveness Framework Study*.

S.S. Solberg Hjorth & Brem, A. M. (2016). *How to Assess Market Readiness for an Innovative Solution: The Case of Heat Recovery Technologies for SMEs*. Sustainability*,* Vol. 2016**,** No. 8, pp. 1-16, doi: 10.3390/su8111152.

TrustArc (2021). *Global Privacy Benchmarks Report*. TrustArc.

Walden, D., Roedler, G., Forsberg, K., Hamelin, D. & Shortell, T. (2015). *Systems engineering handbook of INCOSE*, Wiley.

Wohlin, C., Runeson, P., Host, M., Ohlsson, M. C., Regnell, B. o. & Wessl´en, A. (2012). *Experimentation in Software Engineering*, Springer.

Appendix A: Key project results (KRs)

According to the GA, in order to satisfy its objectives SENTINEL should achieve the following measurable key results.

KR	Measure of success
KR-1.1	Successful integration and orchestration of *SENTINEL* technology offerings.
KR-1.2	40% improved compliance efficiency for SMEs/MEs.
KR-1.3	Reduction of compliance – related costs by at least 40%- against benchmarks defined by stakeholders and EU (International) initiatives.
KR-1.4	30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services from SMEs/MEs all over EU.
KR-1.5	Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility.
KR-2.1	Innovative customized RE-related models deployed with respect to security- and data privacy-aware mechanisms ensuring data protection in SMEs/MEs.
KR-2.2	Accuracy of (distributed) machine (deep) learning algorithms facilitating intelligence in the recommendations for data compliance of more than 80%.
KR-2.3	Test data privacy compliance engine in terms of speed and accuracy.
KR-2.4	Accuracy of data access management and authentication mechanisms offered to SMEs/MEs more than 90%.
KR-2.5	Ensuring the delivery, adoption, and utilization of a unified Identity Management System.
KR-3.1	More than (20) novel services and tools utilised and integrated from diverse multi-domain technological areas and applied in SMEs/MEs environments.
KR-3.2	At least (10) tools and services related to data protection, data privacy management, security assurance and compliance.
KR-3.3	Upgrade ML/DL models to be realised as services in privacy-aware SMEs/MEs environments.
KR-3.4	Accuracy and efficiency of the SENTINEL data privacy compliance recommendation engine at least 70%.
KR-4.1	Successful collection of data for demonstrating automated data privacy and protection compliance procedures in complementary SMEs/MEs environments.
KR-4.2	Delivery of three (3) integrated versions of the SENTINEL framework.
KR-4.3	Execution of five (5) demonstrators in complementary, SMEs/MEs' industries and environments, together validating at least 95% of tools.
KR-4.4	More than ten (10) trials to demonstrate SENTINEL tools' applicability and performance within real-world environments.
KR-4.5	Construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs.

KR	Measure of success
KR-5.1	All SENTINEL solutions, products and services aligned and harmonised with regulations and EU standards.
KR-5.2	Define a concrete dissemination strategy to raise awareness. Uptake more than (6) standards from several data privacy and compliance related technologies.
KR-5.3	More than twenty (20) entities (e.g., academics and enterprises) to use SENTINEL offerings.
KR-5.4	Digital Innovation Hubs engaged to further communicate and support SENTINEL offerings.
KR-6.1	Ready to market integrated solution for the overall security compliance framework and independent data privacy and security enhancing solutions (TRL 7).
KR-6.2	At least four (4) SENTINEL tools reach market readiness level eight (8) at the end of the project.
KR-6.3	At least six (6) third-party collaborations to be established for further applicability verification.
KR-6.4	More than ten (10) critical aspects (e.g., maintenance and software updates) will be addressed to ensure long-term sustainability of the solution.
KR-6.5	A concrete business plan for business continuity (including joint exploitation plans, alliances and collaborations) will be released at the end of the project.

Appendix B: SENTINEL R&I, Business and Dissemination KPIs

According to the GA the KPIs for SENTINEL are organised in three categories as detailed in the following tables.

Research and Innovation KPIs

What the call states	What	How Much?		
		KPIs	Target value	Means of verification
Citizens and SMEs/MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS directive and the application of the General Data Protection Regulation.	***Impact #1:*** Strictly adhered to relevant policies, strategies and activities (GDPR and NIS, ePrivacy etc.) ***SENTINEL*** will deliver an open-access, unified digital architecture enabling both citizens and SMEs/MEs not only improve their data protection, management, and storage but also smoothly fulfil with the mentioned strategies and directives. This will considerably increase the trust and protection of individuals and enterprises to critical ICT systems thus making them potential front-runners in the Digital Single Market	***iKPI1.1:*** Number of privacy and personal data protection technologies delivered	at least 4 (four)	The outcomes of WP2 as reported in D2.1-D2.3
		iKPI1.2: Number of standards, regulations and directive incorporated within ***SENTINEL***	more than six (6)	The outcomes of Task2.1, Task2.5, Task 8.4 as reported in D2.4 and D8.6
		iKPI1.3: (%) Improved privacy compliance efficiency for SMEs/MEs	at least 40%	The outcome of Task 2.2-Task2.4 as reported in D2.1-D2.3
Security, privacy and personal data protection are strengthened as shared responsibility along all layers in the digital economy, including citizens and SMEs/MEs.	***Impact #2:*** The ***SENTINEL*** platform will set up a "one-stop shop" were SMEs/MEs, B2B customer networks, large corporations, cybersecurity actors (CERTs/CSIRTs, DPAs etc.) will be inextricably intertwined. This will significantly enhance security and privacy practices and measures (such as secure data sharing and aggregation,	***iKPI2.1:*** Number of entities CERTS / CSIRTS engaged by the end of the project	more than 20	The outcomes of Task 7.4 as reported in D7.4
		iKPI2.2: Number of Digital Innovation Hubs engaged by the end of the project	more than 8	

What the call states	What	How Much?		
		KPIs	**Target value**	**Means of verification**
	security gaps' identification, data policy matchmaking) by strengthening overall security, privacy and personal data protection among all the involved actors.	***iKPI2.3:*** Number of novel services, tools and modules within the ***SENTINEL*** platform	more than 20	The outcomes of WP3-WP4 as reported in D3.1-D3.3; D4.1-D4.3
Reduced economic damage caused by harmful cyber-attacks and privacy incidents and data (including personal data) protection breaches.	***Impact #3: SENTINEL*** will lead to improved modelling of economic influences on SMEs/MEs and the wider economic impacts of interconnected businesses. The project identifies key economic factors in the SMEs/MEs that are likely to influence performance across the digitally connected ecosystem. This implies greater resilience for the sector as a whole and a greater awareness of vulnerable points in the digital economy.	***iKPI3.1:*** Number of improved business model developed within the ***SENTINEL*** project	**at least** 3	The outcomes of Task 7.1 and Task6.4 as reported in D7.2; D7.6, D6.3
		iKPI3.2: (%) reduction of compliance – related costs	at least 40%	
Pave the way for a trustworthy EU digital environment benefitting all economic and social actors.	***Impact #4:*** Via the envisioned novel "one-stop shop" approach, ***SENTINEL*** will facilitate the establishment of trustworthy and credible EU digital economy via a) rolling out a range of market approaching tools, b) addressing critical aspects in software maintenance and ensure long-term sustainability c) engaging SMEs/MEs in numerous verticals through Digital Innovation Hubs and incubators.	***iKPI4.1:*** Number of tools reach market readiness level eight (8)	at least 4	The outcomes of Task 7.1; Task7.3 as reported in D7.2; D7.5; D7.6
		iKPI4.2: Number critical aspects addressed to ensure long-term sustainability	more than 10	The outcomes of Task 6.4 as reported in D6.4
		iKPI4.3: Number of stakeholders and third parties engaged	10.000 smaller enterprises from at least 6 countries	The outcomes of Task 7.4 as reported in D7.4

Business KPIs

	Expected impact	How Much?		
		KPI	Target	Means of verification
Impact on innovation	**Impact #9:** ***SENTINEL*** supports disruptive innovation in the field of cyber security services for SMEs/MEs; it will provide innovative technologies, solutions and services to these high-risk entities.	***iKPI9:*** Number of innovative technologies advanced within ***SENTINEL***	≥4	The outcomes of WP2 as reported in D2.1-D2.3
	Impact #10: ***SENTINEL*** will directly enhance the innovation capacity to complementary company types within the SMEs/MEs.	***iKPI10:*** Number of cases testing and validating the innovative capacity of the ***SENTINEL’s*** offerings	>5	The outcome of the T 6.2; T 6.3 and T6.4 as reported in D6.1-D6.3
Impact on competitiveness and growth	**Impact #11:** Leveraging state-of-the-art security- and privacy-enhancing modules, ***SENTINEL*** will provide **novel tools and services** for enabling highly automated PDP compliance in SMEs/MEs. This will empower them to enhance their products and strengthen their position in the market.	***iKPI11.1:*** Number of third-party entities (SMEs/MEs) directly using ***SENTINEL***’s tools/services	>20	The outcome of the T7.4 as reported in D7.4
		iKPI11.2: Expected increase of market share for SMEs/MEs exploiting ***SENTINEL***	>10%	The outcomes of T7.1 as reported in D7.2; D7.6
	Impact #12: ***SENTINEL*** is expected to minimise risks associated with digital business initiatives and thus support the development of competitive start-ups and spin-offs	***iKPI12.1:*** Number of start-ups and spin-offs boosted exploiting ***SENTINEL*** security services	>4	The outcome of the T7.4 as report in D7.4
	Impact #13: ***SENTINEL*** will provide significant added value to IT infrastructures of SMEs/MEs.	***iKPI13.1:*** Increase in sales for the pilot partners exploiting ***SENTINEL*** platform	>15%	The outcomes of T7.1 as reported in D7.2; D7.6

Dissemination KPIs

SENTINEL Channels	KPI	Method of measurements	Frequency	Threshold
SENTINEL website	**dKPI#1:** Number of visitors	Google analytics	Monthly	≥ 100
	dKPI#2: Number of page views	Google analytics	Annually	> 5000
	dKPI#3: Number of downloads	Google analytics	Monthly	> 500
Social Media Twitter	**dKPI#4:** Number of followers	Twitter analytics	Monthly	> 20
	dKPI#5: Number of push announcements	Twitter analytics	Monthly	≥20
	dKPI#6: Number of unique	Twitter	Monthly	≥30

SENTINEL Channels	KPI	Method of measurements	Frequency	Threshold
	visitors	analytics		
Social Media LinkedIn	**dKPI#7:** New followers	LinkedIn analytics	Monthly	≥20
	dKPI#8: Number of push announcements	LinkedIn analytics	Monthly	≥20
	dKPI#9: New of unique visitors	LinkedIn analytics	Monthly	≥20
Brand-building materials	**dKPI#10:** Number of distributed hard copies of the ***SENTINEL*** brochure	Direct reporting	End of project	≥1000 distributed in ≥10 events
	dKPI#11: Number of electronic ***SENTINEL*** brochures	Google analytics	End of project	≥1000 downloads
	dKPI#12: Regular newsletters	Admin tool	End of project	≥ 9 newsletters
	dKPI#13: Number of ***SENTINEL*** videos and number of views	YouTube	End of project	3 videos with >1000 views each
Journal & magazine publications	**dKPI#14:** Number of international referred journal publications by ***SENTINEL*** partners	Direct reporting	End of project	>6
	dKPI#15: Number of special issues in international referred journals	Direct reporting	End of project	>2
	dKPI#16: Number of publications in international (printed or online) magazines	Direct reporting	End of project	>6
Presentations in International Conferences	**dKPI#17:** Number of conference presentations by ***SENTINEL*** partners	Direct reporting	End of project	≥ 12
Third-party events (INFO DAYs, workshops, fairs/exhibitions targeting national & EU policy makers, potential stakeholders)	**dKPI#18:** Number of events	Direct reporting	End of project	≥ 15 events with >60 attendees
	dKPI#19: Number of audience contacts	Surveys	End of project	≥50% of the participants
	dKPI#20: Number of participants interested in ***SENTINEL*** project	Surveys	End of project	≥40% of the participants
SENTINEL Events (INFO DAYs, webinars workshops/demonstration events)	**dKPI#21**: Number of events organized by ***SENTINEL*** partners	Direct reporting	End of project	≥ 8 events with ≥60 attendees and 3 events with ≥100 attendees
	dKPI#22: Number of audience contacts	Surveys, interviews	End of project	>=50% of the participants

SENTINEL Channels	KPI	Method of measurements	Frequency	Threshold
	dKPI#23: Number of participants interested in ***SENTINEL*** project	Surveys, interviews	End of project	>=50% of the participants
Liaisons and networking with the other relevant projects	**dKPI#24:** Number of ***SENTINEL*** members actively networking with other relevant projects	Direct reporting	End of project	≥ 6
Standardization/regulation relevant activities	**dKPI#25:** Number of "EAB" members monitoring and ensuring compliance with relevant regulations	Direct reporting	End of project	At least two (2) members of EAB