SENTINEL

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

D6.2 - SENTINEL Demonstration - final execution

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 6
Deliverable Title	D6.2 - SENTINEL Demonstration - final execution
Version	1.8
Date of Submission	30/11/2023
Main Editor(s)	Mihalis Roukounakis (CG), Eleni-Maria Kalogeraki (FP)
Contributor(s)	Siranush Akarmazyan (ITML), Stavros Rafail Fostiropoulos Evangelia Kavakli (IDIR), Thomas Oudin (ACS), Kostantinos Poulios (STS), Dimitris Ntegiannis (STS), Manos Karabinakis (AEGIS), Manolis Falelakis (INTRA), Philippe Valoggia (LIST), George Hatzivasilis (TUC, former TSI), Ruben Costa (UNINOVA), Daryl Holkham (TIG)
Reviewer(s)	Thanos Karantjias (FP), Marinos Tsantekidis (AEGIS)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	31/08/2023	Draft ToC	Confidential
1.1	5/10/2023	Revised ToC	Confidential
1.2	31/10/2023	Partners input collected	Confidential
1.3	3/11/2023	Consolidated version	Confidential
1.4	17/11/2023	Partners input collected	Confidential
1.5	20/11/2023	Consolidated version	Confidential
1.6	22/11/2023	Last updates – Draft ready for Review	Confidential
1.7	28/11/2023	Peer review draft received	Confidential
1.8	30/11/2023	Final version	Public

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
BA	Business Administrator
CG	ClinGenics
CS	CyberSecurity
CSRA	CyberSecurity Risk Assessment
DBS	Disclosure and Barring Service
DC	Dimensions Care
DIH	Digital Innovation Hub
DPIA	Data Protection Impact Assessment
DoA	Description of Action
DPO	Data Protection Officer
EMA	Exome Management Application
FFV	Full-Featured Version
GDPR	General Data Protection Regulation
GDPR CSA	GDPR Compliance Self-Assessment
HPO	Human Phenotype Ontology
HR	Human Resources
ICO	Information Commissioners Office
IIoT	Industrial Internet of Things
IoMT	Internet of Medical Things
KR	Key Result
KPI	Key Performance Indicator
MD	Managing Director
ME	Micro-Enterprise
MS	Milestone
MVP	Minimum Viable Product
N/A	Not Applicable
NDA	Non-Disclosure Agreement
PA	Processing Activity
PDP	Personal Data Protection
PII	Personally Identifiable Information
RM	Registered Manager
RI	Responsible Individual
ROPA	Record Of Processing Activities
SME	Small and Medium Sized Enterprise
TIG	Tristone Investment Group
UX	User Experience
UI	User Interface
WP	Workpackage

Executive Summary

This deliverable has been composed within the context of “WP6 - Real-life experiment evaluations: SENTINEL pilots” and constitutes the main output of “Task 6.2 - Validating SENTINEL offerings to SMEs and MMs: Test cases in the fields of genomics and social care”, “Task 6.3 - Open access to the SENTINEL platform for validation and evaluation through Digital Innovation Hubs” and “Task 6.4 - Evaluation and impact analysis” as presented in the Description of Action (DoA). In particular, the document reports on work carried out regarding the

- Deployment of the SENTINEL test cases in the fields of genomics and socialcare.
- Development of Persona-based Approach.
- Demonstration of the SENTINEL security and privacy offerings as part of Full-Featured Version (FFV) of the SENTINEL platform solution.
- Execution of the trials in an interactive manner over several time-internals.
- Engagement of external actors (SMEs/MEs) via Digital Innovation Hubs (DIHs) to test and validate the offerings of the SENTINEL platform.
- Output collections and further feedback analysis from all real-life demonstrators.

The report is tightly connected with “D6.1 - SENTINEL Demonstration - initial execution and evaluation”, following and extending all pilot and evaluation procedures described. The current deliverable also applies the experimentation protocol initiated in “D1.3 - The SENTINEL experimentation protocol” and refined in D6.1. The deliverable illustrates the demonstration results achieved in the context of SENTINEL Full-Featured Version (FFV) testing activities by presenting and discussing the feedback received from the SENTINEL pilot owners (CG and TIG) and external actors (SMEs/MEs).

It is worth mentioning that the WP6 efforts will be continued also in the remaining project period (M31-M36) by strongly collaborating with additional SMEs/MEs to test the platform and provide feedback to formulate the project’s impact analysis and carry out an overall assessment and evaluation of the final version of the SENTINEL integrated solution as part of Task 6.4 activities. This will be complemented with a series of actions planned for the upcoming period (until M36), including KRs/KPIs assessment for each demonstrator both in operational (cost, service levels, etc.) and technical terms (performance of solution), organization of final workshop by engaging additional SMEs/MEs.

1. Introduction

This deliverable describes working progress of Tasks “T6.2 - Validating SENTINEL offerings to SMEs and MMs: Test cases in the fields of genomics and social care” and “T6.3 - Open access to the SENTINEL platform for validation and evaluation through Digital Innovation Hubs”.

More specifically, it illustrates the pilot workshop demonstration, complete pilots’ execution, and evaluation processes, including evaluation results collection from different target groups to estimate the development progress and integration processes.

As part of Task 6.2 and Task 6.3 activities and by aiming at enhancing the developed Full-Featured Version (FFV) (M18) and proceeding with continuous integration and development activities (Task T5.2) the SENTINEL FFV Demonstration and Validation phases established, as presented in Table 1. Specifically, the table illustrates the execution of these phases, conducted during M19-M30 in parallel to SENTINEL technical development activities (FFV enhancement and final integrated solution). It depicts all three pilot execution processes, including different phases (pilot preparation activities, workshop organisation, trials execution & validation, pilot results analysis) with specific time-internals.

As shown in Table 1, the SENTINEL pilot phases launched in M19. As part of the first Clingenics Pilot (CG pilot), the first SENTINEL FFV Demonstration workshop took place in M22, whereas the trial execution phase occurred during M23-M27. Apart from testing the SENTINEL platform upon specific processing activities identified within the CG pilot at this early stage, the validation aimed at subsequently enhancing the SENTINEL FFV (bug fixes, refinement, better UI/UX attribute addition etc.).

The second pilot of Tristone Investment Group (TIG Pilot) launched in M19 and ended in M29. Aiming to reach out to additional SMEs within the TIG group, this pilot engaged two stages, including the SENTINEL FFV Demonstration workshops (M24 and M29), and respective trials conducted in sequential rounds (between M25 and M28). To this aim, external end-users recruited by TIG, coming from three (3) SMEs in Socialcare (i.e., “Dimensions Care”, “Beyond Limits” and “Sportfit Support Services”).

Finally, the third pilot demonstration workshop of the Digital Innovation Hubs (DIH) realized in M28, although the pilot preparation activities (including DIH engagement, SMEs recruitment, informative/compelling materials creation and distribution) launched in M19. In this SENTINEL Pilot Demonstration workshop, 24 external SMEs participated, including 48 attendees in total. After this event, 10 SMEs/MEs engaged through the workshop, tested and validated the SENTINEL FFV functionalities and provided feedback in M29.

It should be mentioned that, prior to the launch of the FFV testing activities, several preparational activities have been carried out, such as pilot experiments selection, processing activities definition, guidelines and documentation preparation, external end-users’ recruitment and end-user training.

Table 1. SENTINEL FFV Demonstration and validation phases

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="10">Demonstration Phase (M19-M30)</td></tr>
<tr><td>M19-M21</td><td>M22</td><td>M23</td><td>M24</td><td>M25</td><td>M26</td><td>M27</td><td>M28</td><td>M29</td><td>M30</td></tr>
<tr><td colspan="3"></td><td><u>MS4</u>
Demonstration Flame</td><td colspan="5"></td><td colspan="2"><u>MS5</u>
Demonstration Fire</td></tr>
<tr><td rowspan="1">Technical progress</td><td>SENTINEL FFV release</td><td colspan="9">FFV enhancements, technical improvements and continuous monitoring based on end-users’ feedback (M19-30)</td><td>SENTINEL integrated solution final version</td></tr>
<tr><td rowspan="3">SENTINEL Pilots</td><td>CG Pilot</td><td>Pilot Preparation</td><td>Demo Workshop</td><td colspan="3">CG Pilot trials execution, validation</td><td colspan="4">Pilot results analysis</td><td>D6.2</td></tr>
<tr><td>TIG Pilot</td><td colspan="3">Pilot preparation</td><td><u>Part I:</u>
Demo Workshop</td><td colspan="3">Trials execution & validation</td><td><u>Part II:</u>
Demo Workshop for extra SMEs. Trials execution & validation</td><td>Pilot results analysis</td><td rowspan="2"></td></tr>
<tr><td>DIH Pilot</td><td colspan="5">Pilot Preparation</td><td>Demo Workshop</td><td>Pilot trials execution & validation</td><td>Pilot results analysis</td></tr>
</table>

1.1 Purpose of the document

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

1.1.1 Scope

This deliverable establishes the SENTINEL demonstration and evaluation process presenting our approach on profiling users and creating personas, presenting the SENTINEL demonstration execution and evaluation of the platform and suggests a combination of qualitative and quantitative improvements.

1.1.2 Contribution to WP6 and project objectives

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

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

An essential part of WP6 activities was the refinement and finalization of the SENTINEL experimentation protocol, orchestrated by Task 6.1 and initiated under the activities of Task 1.3 and D1.3 [1]. The refined experimentation protocol was reported in D6.1 [2]. The current report describes the three pilots' activities, which applies a part of the SENTINEL experimentation protocol, i.e., pilot planning, pilot execution and an initial analysis of results (a holistic SENTINEL pilots' assessment and impact analysis of the results will be provided in "D6.3 - Assessment report and impact analysis").

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

Aligned with Objective 2, this report details all the activities undertaken for the three SENTINEL pilots: pilot preparations and recruitment activities, the pilot cases and demonstrations, and the end-users' trial executions.

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

The current report provides a description of the pilot validation results retrieved from the three SENTINEL pilots and the presentation of the validation results.

1.1.3 Relation to other WPs Tasks and Deliverables

This document reports on the work carried out within the context of WP6 and mainly describes the outcome of the work performed in "Task 6.2 - Validating SENTINEL offerings to SMEs and MMs: Test cases in the fields of genomics and social care", and "Task 6.3 - Open access to the SENTINEL platform for validation and evaluation through Digital Innovation Hubs". Specifically, Task 6.2 manages and deploys the SENTINEL test cases in the fields of genomics and socialcare, investigating how entities from those fields can increase the levels of data privacy assurance and compliance. Task 6.3 activities focused on exploiting the engagement of external actors (SMEs/MEs) via DIHs to test and validate the offerings of the SENTINEL platform. With this respect, operational trials carried out and SENTINEL security and privacy offerings demonstrated

to a wide range of end-users from several technological domains and with different business needs and requirements. As a result, outputs from all real-life demonstrators collected and analysed to determine the efficiency, operability, usability, robustness, performance, security, and privacy awareness of the pilot demos.

The procedures and methodologies followed for pilot execution and validation, based on instructions described in D6.1 and strictly followed by the SENTINEL partners throughout the pilot demonstration activities.

The pilot evaluation process, described in this report, will drive additional trial executions and the overall assessment of the SENTINEL platform which will be analysed in the deliverable "D6.3 - Assessment report and impact analysis".

Eventually, to deliver a user-centred design of the SENTINEL User Interface (UI) and improve ease-of-use solution, the outputs of pilot execution were thoroughly examined and considered in the final release of SENTINEL visualisation and UI component. Deliverable D5.3 [3] reports on the collected input, considered to further update, improve, and expand the UI component towards the final prototype version, according to the end-user needs.

1.2 Structure of the Document

The current deliverable is structured as follows:

- Section 1 - "Introduction" gives an overall presentation of the current document.
- Section 2 - "Pilot evaluation aspects" describes the persona-based approach followed and gives updates and enhancements on the User Evaluation Questionnaires.
- Section 3 – "Pilot 1: ClinGenics Pilot (CG Pilot)" describes the CG Pilot preparation, execution, and results elaborations.
- Section 4 – "Pilot 2: Tristone Investement Group Pilot (TIG Pilot)" describes the TIG Pilot preparation, execution, and results elaborations.
- Section 5 – "Pilot 3: SMEs/MEs engaged via DIH (DIH Pilot)" describes the DIH Pilot preparation, execution, and results elaborations.
- Section 6 – "SENTINEL pilot evaluation outcomes, KRs/KPIs progress and monitoring" reports on the overall validation results, KRs/KPIs progress and monitoring.
- Section 7 – "Conclusion and next steps" summarises this deliverable with conclusions and future steps.

1.3 Intended readership

The deliverable is intended for both consortium members and stakeholders, external to the project. primarily addressed to SMEs and MMEs, since the dissemination level of D6.2 is public. This document is a guide to both consortium members and external readers to understand the SENTINEL execution and evaluation process.

2. Pilot evaluation aspects

Aiming at assisting the design of user experiments and guiding the identification of UI/UX improvements, the SENTINEL persona-based approach has been defined and elaborated in this section.

2.1 Following a persona-based approach

Understanding the users' needs is important for developing an application that provides good usage experience. To address this, personas can be developed as user representations to provide a comprehensive understanding of the user, and to stimulate empathy, building a common vision for the targeted users among the project team members.

A persona is a hypothetical archetype of a real user that describes the user's goals, skills, and interests [4]. Personas aid in creating user-centred designs whereby design choices are guided by the needs and expectations of the personas, ensuring that the system caters to a diverse user base. They can be used both in the early stages of system development to guide the identification of user requirements, as well as during testing and validation to test the system against varied user behaviours, ensuring a more robust and comprehensive evaluation.

In SENTINEL, the persona-based approach is used during the SENTINEL testing and validation of the FFV for assisting the design of user experiments and for guiding the identification of UI/UX improvements. In the first case, personas aid in the creation of scenarios that represent how different personas might interact with the system, whilst in the latter personas will aid in rethinking the user flows and define appropriate user help that best suits the requirements of the diverse groups represented by the personas.

Identifying personas involves the following steps:

1) *Gather Data*: Collect information about the potential users. This can be done through interviews, surveys, observations, or questionnaires, aiming to get insights into the user demographics, behaviors, preferences, and pain points that will help developers understand and empathize with this user.

2) *Identify Patterns and Commonalities*: Analyse the data collected and look for common characteristics, behaviors, and goals among the users. Identify patterns and group similar traits together.

3) *Create Persona Profiles*: Develop detailed personas based on the identified patterns and commonalities. These can be communicated using visual or text-based representations.

The above process can be assisted by the use of templates composed by appropriate fields for obtaining persona attributes. The template used in SENTINEL is based on the PATHY technique [5] [which consists of six fields (Who, Context, Technology experiences, Problems, Needs, and Existing solution) that describe the persona’s characteristics, the environment they engaged in, their technical proficiency, the problems they are facing and how they want to solve them, and current problem-solving options (see Figure 1).

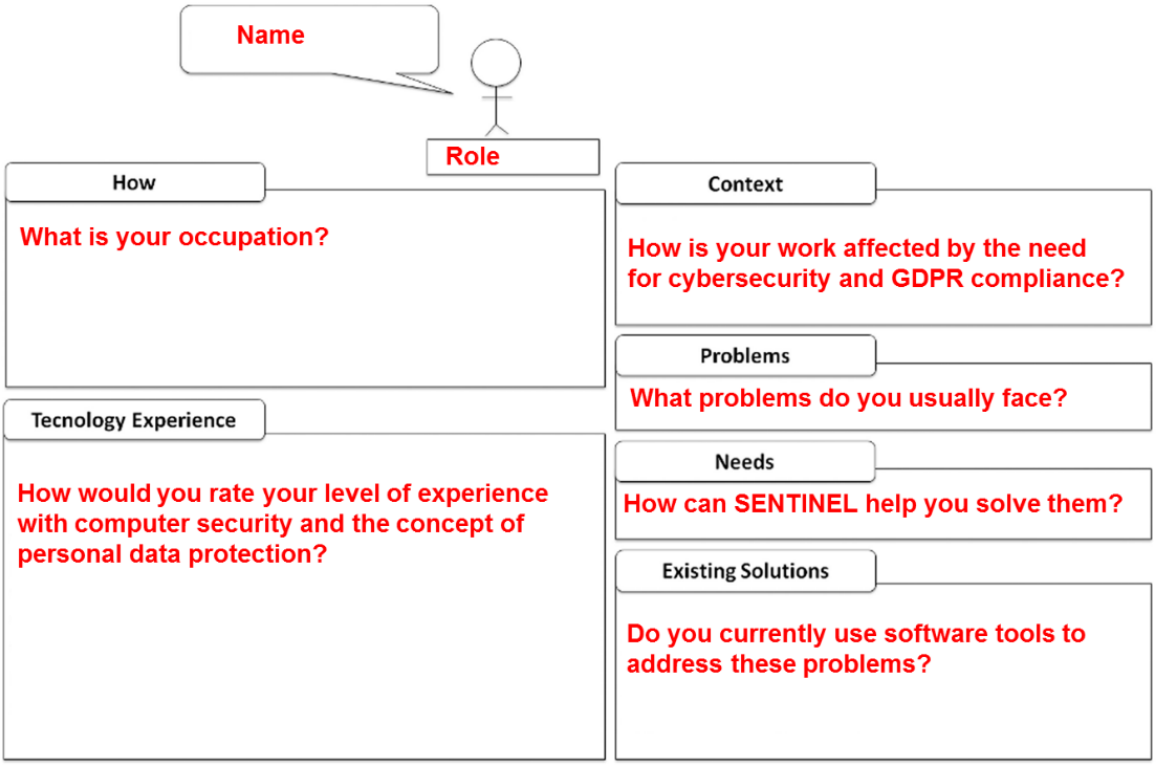


Figure 1. The persona template used in SENTINEL based on the PATHY technique

As shown in Figure 1, each field has guiding questions relevant to SENTINEL platform design that should be answered based on information collected from users.

The main instrument for collecting information form users has been the user evaluation questionnaires filled by SENTINEL users participating in the 3 pilot cases. In particular, the user evaluation questionnaire has been used during testing and validation of the 1st FFV version, by the SME users of the CG (2 end-users) and TIG (4 end-users) engaged by a focused pilot case and an additional generic case (cf. Sections 4.6, 4.7). Further, 10 SME/ME users have filled-in the questionnaire in the context of the 3rd DIH pilot case on external SMEs/MEs.

Additional information regarding users has been collected during the 3 SENTINEL Demonstration Workshops.

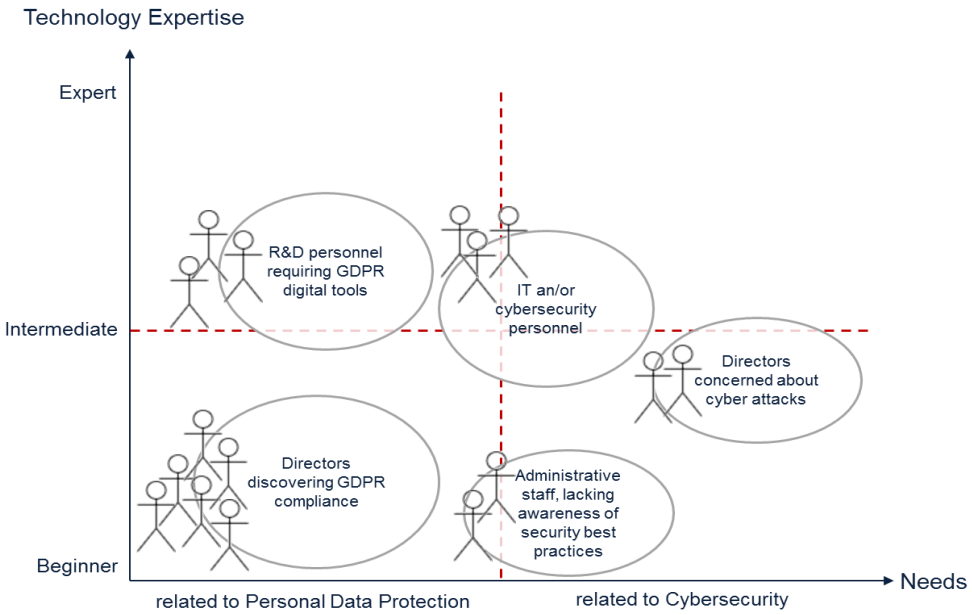


Figure 2. SENTINEL personas

Analysis of the data collected has revealed several commonalities between user attributes based on their technology expertise, and needs, as shown in Figure 2. This grouping indicates common patterns which can be associated with the design of alternative workflows associated with each user group each comprised of the functionalities that better suit user requirements, as shown in Table 3.

Table 2. Associating user personas to SENTINEL functionalities

Persona description	**Required SENTINEL functionalities**
SME administrative staff discovering GDPR compliance	Creation of PAs, Use of ROPA, Acquire policy recommendations (O6 Data protection recommendations)
SME R&D personnel requiring GDPR digital tools	Creation of PAs, Use of ROPA, GDPR Compliance Self-Assessment, Data Protection Impact Assessment. Acquire policy recommendations (All recommendations)
SME IT personnel responsible for achieving GDPR compliance	Cybersecurity Risk Analysis (CSRA/Mitigate, Cyber-assets, CyberRange, Threat Intelligence), Exploring the Observatory, Reporting incidents
SME IT / cybersecurity personnel	Cybersecurity Risk Analysis (CSRA/Mitigate, Cyber-assets, CyberRange, Threat Intelligence), Exploring the Observatory,

	Reporting incidents
SME administrative staff lacking awareness of security best practices	Cybersecurity Risk Analysis (Gamified CyberRange SME scenarios)

This association of user personas to required SENTINEL functionalities can guide both the design of customised user workflows for the FFV final version as well as the provision of tailored user guidelines and help (manuals).

2.2 Updates and enhancements on SENTINEL User Evaluation Questionnaire

According to the SENTINEL experimentation protocol described in deliverables D1.3 and D6.1, the experimentation process is an iterative and incremental procedure, often requiring the alignment of the experiments' definition and the adjustment of the evaluation instruments used to best reflect pilot requirements as well as to be in line with the technical updates of the SENTINEL platform. As a result, several revisions have been made to the SENTINEL user evaluation questionnaire.

As mentioned in section 2.1, the questionnaire is the main instrument for collecting information and identifying user personas. To this end, the original questionnaire has been adjusted, adding new questions when necessary, in order to reflect the 6 fields of the persona template. The following Table 3 shows the correspondence between the fields of the personal template and the questions of the revised user evaluation questionnaire.

Table 3. Correspondence between persona template and questions in the user evaluation questionnaire

Template field	**Relevant question(s)**
How	Q3. What is your current position in the organization
Technology Expertise	Q4. What is your area of expertise Q5. Please identify your level of expertise regarding cybersecurity. Q6. Please identify your level of expertise regarding personal data protection and EU GDPR compliance regulation?
Context	Q7. Are you currently involved in performing or assessing cybersecurity, privacy or personal data protection processes in your organisation? Q8. Please specify your involvement and related tasks.
Existing Solution:	Q9. Does your organisation employ any tools or services for privacy assessment to estimate and/or support its GDPR compliance?
Problems	Q15. Please summarise any specific concerns you have about cybersecurity and personal data protection in your organisation.
Needs	Q16. How do you believe that the SENTINEL platform can help to resolve your concerns?

Additional revisions were also deemed necessary aiming to:

(a) incorporate users' comments involved in the CG and TIG pilot cases, regarding:
   a. clarification of existing questions (e.g., Q9 and QB2)

b. improving alignment between questions and SENTINEL functionality (see QA1.1 and QA1.7)

c. addition of open-ended questions that allow respondents to provide feedback in their own words thus assisting them to further elaborate on their experience of the SENTINEL platform and provide detailed feedback (see questions QA1.10, QA2.12, QA3.5)

(b) include specific questions for the evaluation of the CyberRange Game (see questions QA3.1 – QA3.5).

(c) provide questions that clarify SENTINEL impact on Business Performance (see QA6.11 and QA6.12).

(d) reflect the requirements of the DIH pilot case involving external SMEs, by removing specific references and details that limit the applicability of questions to the specific Processing Activities (PA) of the previous pilots and to accommodate alternative experiment scenarios (use default PAs provided in the platform, use custom PAs, use both), as new section “Experimental Details”.

The final User Evaluation Questionnaire highlighting the above revisions is provided in Appendix-I. and falls into seven (7) main sections:

- **User Details** *(focusing on user details and managerial, economic and privacy aspects of the organisation)*
- **User Satisfaction** *(questions mostly based on ISO/IEC 25010 [6] quality metrics, such as Learnability, Usability, Time Efficiency, Functional Suitability and System Performance)*
- **User Interface/User Experience** *(UI/UX)*
- **CyberRange Gaming** *(Simulation service for Cybersecurity hands-on training)*
- **Security and Results Quality, Personal Data Protection and Compliance**
- **Business Performance** *(Evaluate, according to end-user business needs)*
- **Express end-user opinion and additional comments** *(allow the users to provide textual feedback to further express their comments after experiencing SENTINEL and provide suggestions for improvements)*.

3. Pilot 1: ClinGenics Pilot (CG Pilot)

CG Pilot represents the first pilot of SENTINEL, accomplished by ClinGenics (CG) in the early FFV version of the SENTINEL platform. This section describes the objectives, pilot overview, the experiments' workflow, the pilot preparation procedures and the workshop for the SENTINEL demonstration to the CG end-users. Furthermore, it illustrates the execution and the evaluation results because of specific experiments conducted during the pilot execution process.

3.1 Pilot Objective

The CG pilot aimed at testing and validating the SENTINEL FFV functionalities under real-life operation scenarios in the context of ClinGenics normal operations and especially Exome Management Application (EMA). The purpose of the pilot operations was to gather feedback from the CG end-users considering their personal experience after performing the trials in the frame of two (2) experiments, as described in Section 3.5.1.

3.2 Pilot Overview

The CG Pilot Case refers to ensuring security and privacy of genomic and of user/client data when using EMA, which is a hybrid web app with Sensitive but not Personal Data. The following table summarizes the CG pilot case, presented in D6.1.

Table 4. CG Pilot Case: Healthcare

Case overview	**Ensure security and privacy of genomic and of user/client data**
Case company	ClinGenics Ltd. (UK)
Business context	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	Exome Management Application (EMA) 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 several 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.
Type of Data	• **Human DNA sequence variants**: vcf file format (https://github.com/samtools/hts-specs) generated typically by NGS applications, submitted by the users for variant prioritization and interpretation. • Standardized, in **Human Phenotype Ontology (HPO) format**: phenotype/disease-related information accompanying the specific co-submitted vcf data file. • Simple **anonymous proband demographic data**, e.g., gender, age, ethnicity, disease status (affected or not) and relevant disease inheritance information. • **Technical/experimental data associated with the type of NGS** analysis, platform utilized, etc.

	• **Internal database** containing **user/customer-related information submitted during registration**, e.g., name, occupation, institution/affiliation, telephone, and email for obvious administrative purposes.
Pilot Operation expectations	To ensure: **(a) Personally Identifiable Information (PII) during the submission process** (b) **Cybersecurity protection of all stored data, etc.**

As reported in D6.1, CG has undertaken two experiments each one engaging a different processing activity, summarized in Table 5 and Table 6 and further presented in Section 3.5.1.

Table 5. CG Pilot 1st Experiment overview

Experiment name	**Security of user/client data**
Experiment Description	ClinGenics realize the processing activity of collecting data for marketing and Sales. The current activity incorporates the following operational procedures: Contact via phone or email and get personal details (i.e., name, surname, job title, email, phone, notes, etc.). Store information to local database (MySQL) and Backup Data to external storage
SENTINEL platform	All SENTINEL functionalities, components and plugins
Processing Activity (PA)	Collect data for Marketing and Sales
Experiment's Variables	Business: Service/product quality, Reliability (Availability), Maintainability (Reusability), Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization) CS & PDP: Compliance, Security (Threat Containment, Data Breach Prevention)
Experiment's Goals	Use the SENTINEL platform to assess the privacy and security of data collected for marketing and sales and receive recommendations on OTMs to ensure user/client data privacy and security. Validate the efficiency of SENTINEL in ensuring user/client data privacy without negatively affecting CG productivity. Finally make recommendations about the Sentinel FFV User Interface and the overall User eXperience.
Logistics *(Participants and type of users/Pilot Duration/Pilot Location/Others)*	User roles: CG Administrator, IT Manager Number of participants (individual users): two (2) Pilot assets: Hardware and Software examined. • Local Storage: Workstation (OS: win10) and external drives for backup purposes. • Cloud web services: GoDaddy.com Database server (MySQL). • Email services: Gmail
Experiment Workflow	**Step1:** Use the SENTINEL platform to investigate the level of GDPR compliance, privacy, and cybersecurity of the PA: "Collect Data for Marketing and Sales", including its operating assets. Receive a set of tailor-made privacy and security policies and services. To execute this step of the experiment, a set of use cases may be executed in the SENTINEL platform sequentially as presented here:

	• Organisation Profiling • Completing an assessment workflow • Acquiring policy recommendations **Step2:** Explore policy monitoring services and consult SENTINEL to gather up-to-date information for policy implementation, application of controls and further privacy and security information. To implement the current step of the experiment, a set of use cases may be executed in the SENTINEL platform sequentially analysed in the following: • Policy monitoring • Browsing the observatory • Reporting incidents
Test cases	All SENTINEL Use cases
KPIsKRs *(where applicable)*	*KR-1.2: 40% improved compliance efficiency for SMEs/MEs* Reflective variables: Compliance (Conformance) *KR-1.4: 30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU.* Reflective variables: Service/product quality, Reliability (Availability), Maintainability (Reusability), Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization) *KR-1.5: Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility.* Reflective variables: Security (Threat Containment, Data Breach Prevention)

Table 6. CG Pilot 2nd Experiment overview

Experiment name	**Proactive Security of genomic data**
Experiment Description	Evaluate Sentinel Platform CS and PDP capabilities in terms of assessing the security and privacy (CSRAnt, GDPR compliance, DPIA) of the EMA data submission processing activity (and its related pilot assets) and explore/review suggestions/recommendations on privacy and security measures (OTMs).
SENTINEL platform	All functionalities of SENTINEL components and plugins
Processing Activity (PA)	Exome Web Application. Collect, compare, and process genetic data from professionals. Relevant Gene Variant Identification. Identifying the variant(s) of potential causative effect
Experiment's Variables *(where applicable)*	Business: Service/product quality, Reliability (Availability), Maintainability (Reusability), Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization) CS & PDP: Compliance, Security (Threat Containment, Data Breach Prevention)
SENTINEL Experiment's Goals	Assess the efficiency of SENTINEL in improving privacy and secure access of genomic data without negatively affecting CG productivity.
Logistics *(Participants and type of users/Pilot Duration/Pilot Location/Others)*	User roles: CG Administrator, IT Manager Number of participants (individual users): two (2) Pilot assets: Hardware and Software to be examined. • Local Storage: Workstation (OS: win10) and external drives for backup purposes. • Cloud web services: GoDaddy.com server (Ubuntu).

	• Cloud web services: GoDaddy.com Database server (MySQL). • EXOME java local application (java_se:11.0.3)
Experiment Workflow	**Step1:** Use the SENTINEL platform to investigate the level of GDPR compliance, privacy, and cybersecurity of the PA: "Collect Data for Marketing and Sales", including its operating assets. Receive a set of tailor-made privacy and security policies and services. To execute this step of the experiment, a set of use cases may be executed in the SENTINEL platform sequentially as presented here: • Organisation Profiling • Completing an assessment workflow • Acquiring policy recommendations **Step2:** Explore policy monitoring services and consult SENTINEL to gather up-to-date information for policy implementation, application of controls and further privacy and security information. To implement the current step of the experiment, a set of use cases may be executed in the SENTINEL platform sequentially analysed in the following: • Policy monitoring • Browsing the observatory • Reporting incidents
Test cases	All SENTINEL Use cases
KPIs/KRs *(where applicable)*	*KR-1.2: 40% improved compliance efficiency for SMEs/MEs* Reflective variables: Compliance (Conformance) *KR-1.4: 30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU.* Reflective variables: Service/product quality, Reliability (Availability), Maintainability (Reusability), Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization) *KR-1.5: Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility.* Reflective variables: Security (Threat Containment, Data Breach Prevention)

3.3 Pilot plan and Demonstration setup

As part of WP6 activities a concrete plan was prepared (see Table 1This deliverable describes working progress of Tasks "T6.2 - Validating SENTINEL offerings to SMEs and MMs: Test cases in the fields of genomics and social care" and "T6.3 - Open access to the SENTINEL platform for validation and evaluation through Digital Innovation Hubs".

More specifically, it illustrates the pilot workshop demonstration, complete pilots' execution, and evaluation processes, including evaluation results collection from different target groups to estimate the development progress and integration processes.

As part of Task 6.2 and Task 6.3 activities and by aiming at enhancing the developed Full-Featured Version (FFV) (M18) and proceeding with continuous integration and development activities (Task T5.2) the SENTINEL FFV Demonstration and Validation phases established, as presented in Table 1. Specifically, the table illustrates the execution of these phases, conducted during M19-M30 in parallel to SENTINEL technical development activities (FFV enhancement

and final integrated solution). It depicts all three pilot execution processes, including different phases (pilot preparation activities, workshop organisation, trials execution & validation, pilot results analysis) with specific time-internals.

As shown in Table 1, the SENTINEL pilot phases launched in M19. As part of the first Clingenics Pilot (CG pilot), the first SENTINEL FFV Demonstration workshop took place in M22, whereas the trial execution phase occurred during M23-M27. Apart from testing the SENTINEL platform upon specific processing activities identified within the CG pilot at this early stage, the validation aimed at subsequently enhancing the SENTINEL FFV (bug fixes, refinement, better UI/UX attribute addition etc.).

The second pilot of Tristone Investment Group (TIG Pilot) launched in M19 and ended in M29. Aiming to reach out to additional SMEs within the TIG group, this pilot engaged two stages, including the SENTINEL FFV Demonstration workshops (M24 and M29), and respective trials conducted in sequential rounds (between M25 and M28). To this aim, external end-users recruited by TIG, coming from three (3) SMEs in Socialcare (i.e., “Dimensions Care”, “Beyond Limits” and “Sportfit Support Services”).

Finally, the third pilot demonstration workshop of the Digital Innovation Hubs (DIH) realized in M28, although the pilot preparation activities (including DIH engagement, SMEs recruitment, informative/compelling materials creation and distribution) launched in M19. In this SENTINEL Pilot Demonstration workshop, 24 external SMEs participated, including 48 attendees in total. After this event, 10 SMEs/MEs engaged through the workshop, tested and validated the SENTINEL FFV functionalities and provided feedback in M29.

It should be mentioned that, prior to the launch of the FFV testing activities, several preparational activities have been carried out, such as pilot experiments selection, processing activities definition, guidelines and documentation preparation, external end-users’ recruitment and end-user training.

Table 1) for each Pilot cases that was followed during the SENTINEL real-world demonstration phase. It should be mentioned that prior to the launch of the FFV testing activities, several preparational activities have been carried out such as definition of experiments, guidelines and documentation preparation, external end-users’ recruitment and end-user training.

Following the same paradigm used in MVP testing activities before CG pilot launch the CG end-users were invited to Demonstration Workshop (M22) to assist them to understand what the SENTINEL solution is (scope, functionalities, the use cases etc.), and how to test it. Starting from M23, the CG end-users get used to the FFV of the SENTINEL platform and start testing the platform by completing the experiments described previously.

Right after the trial execution the given questionnaires forms were submitted as well as an excel data sheet was used to collect and categorize UI and UX suggestions. Similarly, during July and August, the CyberRange part was tested and validated.

3.4 SENTINEL FFV Demonstration Workshop

In the context of the CG Pilot, the SENTINEL Demonstration Workshop carried out at 28th of March 2023 (M22) aiming to acknowledge the CG pilot environment, demonstrate the FFV of the SENTINEL platform and indicate the testing and validation processes for the SENTINEL trials execution and evaluation to CG pilot end-users.

As shown in the workshop agenda (Figure 3) the entire duration of the Demonstration workshop was 2 hours. More than 15 people attended the workshop, including participants of three (3) CG representatives and the SENTINEL project partners.

	CG Pilot: SENTINEL Demonstration Workshop **28 March 2023** **Duration: 15.00-17.00 CET** **Moderator: ITML**	
15.00 – 15.10	Opening & Welcome – SENTINEL Project Overview	**ITML**
15.10 - 15.30	Data Security and Data Protection as enablers for creating value from data	**LIST**
15.30 - 15.45	CLINGENICS Company and genomics data	**CG**
15.45 - 16.00	The EXOME platform, technologies utilised and data collected.	
16.00 - 16.30	CG Pilot – SENTINEL Hands-on training	**INTRA**
16.30 - 16.40	Definitions to end-users on SENTINEL trial execution and evaluation process	**ITML, FP**
16.40 - 17.00	Q&A	**CG End-Users, SENTINEL partners**

Figure 3. CG pilot: SENTINEL Demonstration workshop genda

The main actors of the SENTINEL Demonstration Workshop are presented in the following:

Moderator: the workshop coordinator who initiates the workshop, presented the topics of the agenda and took care of its smooth and timely operation. In addition, the moderator was responsible for recording the workshop after reaching consensus of all attendees and monitoring the Q&A session.

Project Presenters: the project partners who undertook the responsibility to:

- share knowledge to the workshop participants on topics of GDPR, privacy and data protection.

- present the SENTINEL FFV functionalities and train the participants for the trials execution.
- provide guidance for the trials execution and evaluation processes and inform about the training and education material utilized for this process.
- record the observations and suggestions.

Participants: CG participants who attended the SENTINEL FFV hands-on training workshop. They presented their company and personal data handling normal operations to liaison with SENTINEL project partners. They were asked to “think aloud” and interact during the workshop sessions and share their thoughts, suggestions etc.

Tasks: The tasks were activities requested by the CG workshop participants to perform:

- try the SENTINEL FFV functionalities via the implementation of the presented experiments and assess them under specific evaluation criteria, such as, usability, performance, user satisfaction, UI, UX, time efficiency and quality at specific time period.
- assess the SENTINEL FFV functionalities, according to the specific SME’s needs for CS and PDP.
- Fill in the SENTINEL User Evaluation online questionnaire (see Appendix -I) and provide additional feedback/suggestions for improvements after completing the trials.

3.5 The SENTINEL FFV Experiment

In this section, the purpose and workflow of the CG pilot experiments are presented.

3.5.1 Purpose of the SENTINEL FFV Experiment

The CG trial execution phase carried out after the Demonstration Workshop from M23 to M27. During this period, two end-users, as presented in Section 3.2, conducted trials to validate the SENTINEL platform (accessed online via https://platform.sentinel-project.eu/) under the scope of two (2) focused experiments.

The purpose of conducting the trials through these experiments was to engage SME end-users to try and validate the FFV of the SENTINEL platform from a twofold perspective:

- to test and validate the available functionalities of the SENTINEL FFV under real-life operation scenarios and provide feedback considering their personal experience gained after performing the trials considering validation criteria, such as, usability, performance, user satisfaction, UI/UX, speed, flexibility, quality, efficiency.
- to test the way that SENTINEL FFV addresses privacy, personal data protection and cybersecurity requirements of different PAs performed in the context of CG normal operations.

To execute the trials, educational and training material was available to them, such as the Demonstration Workshop recording and the CG Pilot instructions. After completing the trials in

the SENTINEL platform, CG end-users completed two online User Evaluation Questionnaires for the main SENTINEL functionalities, and the CyberRange Gaming simulation environment respectively. The reason of preparing two different questionnaires was that by the time the CG trials commenced (M23) the CyberRange simulation environment was not ready yet. In this regard, CyberRange was tested during M25-M27.

The content of the CyberRange questionnaire was slightly updated to the objectives described in Section 2.2 and incorporated in the final version of the User Evaluation Questionnaire (cf. Appendix-I). Moreover, instead of the questionnaire-based evaluation, a CG end-user provided detailed textual evaluation feedback for the SENTINEL functionalities via an excel evaluation form (cf. D6.1). The CG pilot results derived from both evaluation means are described in Section 3.6.

The SENTINEL FFV tested by the CG trials provides an end-to-end digitalised, user-friendly GDPR [7] and data protection compliance framework for self-assessment based on the established process assessment principles defined in ISO/IEC 33001 [8] and offers a set of cybersecurity services. In particular, the SENTINEL user followed subsequent steps (presented in Section 3.5.2 and further analysed in the instructions document, i.e., Appendix-II) provide information concerning:

- SME's organisational data.
- SME's PAs of personal data (including assets operating).
- SME's privacy and cybersecurity measures implemented.

Afterwards, the SENTINEL platform estimated the level of GDPR compliance, privacy, personal data protection per PA and for the SME overall and identified cybersecurity assessment results on the PAs assets. Furthermore, it delivered a set of tailor-made privacy and security policies and capabilities for their monitoring, implementation and additional services aimed at SENTINEL user increasing the end-user's privacy and cybersecurity awareness.

Data related to the organisation's PAs are primarily important as they provide the appropriate material which is to be assessed for establishing the necessary GDPR compliance checks and impact assessments. Details of the CG pilot experiments are depicted in the following Table 7.

Table 7. CG processing activities overview

Pilot Experiment	Processing Activity (PA)	Experiment's Goal
1st experiment: "Security of user/client data"	"Collect data for Marketing and Sales"	Use the SENTINEL platform to assess the privacy and security of data collected for marketing and sales and receive recommendations on OTMs to ensure the user/client data privacy and security.
2nd experiment: "Proactive security of genomic data"	"Exome Web Application"	Use the SENTINEL platform to assess the privacy and security of personal data created/managed /processed/ transferred via Exome Web Application and deliver recommendations to improve privacy and ensure the secure (authorised) access of genomic data.

Those experiments and the respective PAs are related to CG sector-specific topics on genomics Healthcare and SMEs general operations.

The **"Collect Data for Marketing Sales"** PA is executed via:

- phone or via email
- verbal or written description of the data collection
- the processing activities verbal consent of the subject or by email

The "**Exome Web Application"** PA refers to CG's tested bioinformatics platform-pipeline coupled to expert manual curation, for the prioritisation, evaluation and reporting of actionable genomic variants. The EMA-Exome Management Application is intended exclusively for clinicians and genetics professionals who need a tested and reliable decision/support/advisory tool to aid in their clinical investigations and diagnosis of patients subjected to clinical exome sequencing studies.

3.5.2 SENTINEL Use Cases and Experiments Workflow

The CG Pilot experiments followed a subsequent step-based approach, presented in the following:

Step 0. Register/Sign in the SENTINEL platform

Step 1. Utilise the SENTINEL platform to investigate the level of GDPR compliance, privacy, and cybersecurity of the under-examination PA, including its operating assets. Receive a set of tailor-made privacy and security policies and services.

Step 2. Explore policy monitoring services and consult SENTINEL to gather up-to-date information for policy implementation, application of controls and further privacy and security information.

Step 3. Explore the CyberRange Gaming simulation environment for cybersecurity hands-on training.

Each step was realized via a set of SENTINEL use cases described next. After each use case description, a table is displayed to illustrate the paths that followed on the SENTINEL platform to perform the use case. Indicative screens of the SENTINEL platform were depicted in the instructions detailed document which allowed the user to better comprehend how to implement each specific use case. Analytical description of the SENTINEL Use Cases is provided in the generic SENTINEL End-User Instructions (cf. Appendix-II) as well.

Before performing each of the two experiments, registration needed by the CG representatives accessing the SENTINEL platform for the first time and signing in after creating a user account (Step 0).

Once, SENTINEL registration (Step 0) accomplished, step 1 can be executed by trying and testing the following high-level use cases of the SENTINEL FFV. The SENTINEL use cases are extensively presented in the SENTINEL instructions (cf. Appendix-II).

Organisation Profiling

- **Basic organisation** data (Organisation/Company name, sector, country, size)

- **Details of contact persons responsible for the protection of personal data** in this organization
- **Generic (organization-wide) asset profile**: asset ownership (owned/not owned), asset deployment model [locality] (on-premises/cloud/hybrid)
- **Cyber expertise level**: Beginner, Intermediate, Expert
- **Asset Inventory:** Creating individual asset profiles, including relationships with other assets, PAs and OTMs
- **Processing Activities (PAs):** Information regarding the handling of personal data, represented as a provisional list of PAs and their details.

The Organisation Profiling Use Case workflow is presented in Table 8.

Table 8. Organisation Profiling Workflow

"Organisation Profiling"
SENTINEL implementation paths ➢ Sentinel Dashboard Menu -> My Organisation -> Basic Data ➢ Sentinel Dashboard Menu -> My Organisation -> Contacts ➢ Sentinel Dashboard Menu -> My Organisation -> Generic Asset Profile ➢ Sentinel Dashboard Menu -> My Organisation -> Asset Inventory ➢ Sentinel Dashboard Menu -> Data Protection -> Processing Activities -> Processing Activity -> Commit to ROPA ➢ Sentinel Dashboard Menu -> Data Protection -> Processing Activities -> ROPA

Completing an assessment workflow: The system evaluated the developed DC organisation offered assessment workflows and implementing progressively three types of assessments:

- **The GDPR Compliance Self-Assessment (GDPR CSA)** to determine the compliance level for the under-examination PA and for the entire organisation.
- **The Data Protection Impact Assessment (DPIA)** to determine the data protection impact, likelihood and privacy risks per experiment's PA.
- **The Cybersecurity Risk Assessment (CSRA)** engaging in the SENTINEL Dashboard Menu additional functionalities, i.e., the attack simulation environment to allow the DC end-users to experiment on several cyber-attack scenarios towards registered cyber-assets.

The current Use Case workflow is presented in Table 9.

Table 9. Completing an Assessment Workflow

"Completing an assessment workflow"
SENTINEL implementation paths **GDPR Compliance Self-Assessment:** ➢ Sentinel Dashboard Menu -> Data Protection -> Processing Activities -> GDPRC **Data Protection Impact Assessment:** ➢ Sentinel Dashboard Menu -> Data Protection -> Processing Activities -> DPIA

Cybersecurity Risk Assessment:
- Sentinel Dashboard Menu -> Data Protection -> Processing Activities -> CSRA

Review assessment results:
- Sentinel Dashboard Menu -> Data Protection -> Processing Activities

Cybersecurity simulation environment:
- Sentinel Dashboard Menu -> Cybersecurity -> Simulation Environment

Acquiring Policy Recommendations: The output of the assessment workflows, used by the system in the current use case to acquire policy recommendations. Especially the risk assessment levels produced, i.e., privacy (DPIA results) and security (CSRA results) risk levels, are crucial for the effective operation of the Policy Recommendations. End-users receive a set of tailor-made human-readable and actionable policy recommendations both at organisational level (global) and at PA level containing:

- OTMs to be implemented.
- Proposed tools (plugins) to be employed.
- educational and training material to be studied by SME's staff corresponding to the SME profile parameters and proportional to the calculated risk level for both the organisation as a whole and its individual Pas of personal data.

This Use Case workflow is presented in Table 10.

Table 10. Acquiring Policy Recommendations

"Acquiring Policy Recommendations"
SENTINEL implementation paths **Review assessments results** ➢ Sentinel Dashboard Menu -> Policy -> Recommendations -> Assessments **Review recommendations** ➢ Sentinel Dashboard Menu -> Policy -> Recommendations -> Recommendations

Once step 1 is performed, the following SENTINEL Use Cases are undertaken to support the implementation of step 2.

Policy Monitoring: Tracks the implementation status of the OTMs contained in the policy draft presented previously (cf. Table 11).

Table 11. Policy Monitoring

"Policy Monitoring"
SENTINEL implementation paths ➢ Sentinel Dashboard Menu -> Policy -> Recommendations -> OTM

Browsing the observatory: The SENTINEL Observatory is the platform's intelligence knowledge hub that mainly responds to savvy end-users providing them with rich content on the latest cybersecurity threats and vulnerabilities collected from external sources. The MISP threat sharing platform collects, stores and shares cybersecurity indicators and threats for cybersecurity

incidents and malware analysis. By browsing its list, the user can select types of threats that may be the organization vulnerable and view all the updated information regarding each Indicator of Compromise.

Reporting Incidents: The SME representative may use the SENTINEL platform to report and share with appropriate response teams and/or open security data platforms (e.g., malware information sharing and incident response hubs) a security incident that may have been detected to the organisation. To this end, the SENTINEL platform provides a form which may be used to include all necessary information and submit it to proper external bodies. The format used is based on MISP to assure maximum compatibility.

Table 12. Browsing the Observatory

"Browsing the Observatory"
SENTINEL implementation paths ➢ Sentinel Dashboard Menu -> Observatory -> Knowledge Base -> Vulnerabilities ➢ Sentinel Dashboard Menu -> Observatory -> Knowledge Base -> Threats ➢ Sentinel Dashboard Menu -> Observatory -> Threat Intelligence ➢ Sentinel Dashboard Menu -> Observatory -> Threat Intelligence -> Report Incident

At last, in step 3 the end-user can additionally explore the CyberRange gaming simulation environment for cybersecurity hands-on training. The CyberRange use case is presented in the following.

CyberRange Gaming: The SENTINEL CyberRange Airbus gaming interface is an external simulation service for Cybersecurity hands-on training. AIRBUS provides a new training approach with a Gaming interface based on the CyberRange in order to raise awareness. The users learn in an interactive way the best practice to better protect personal and sensitive data.

During the trial the end-users saw how to connect to the Gaming interface and start the mission. They learned how to interact with the platform and validate the objectives to fulfil the mission. The score they get was 100 /100 and completed in less than 2 hours. Respectively, CG end-users evaluated CyberRange via online Questionnaire-based form and excel data sheets, presented in Section 3.6.8.

Table 13. CyberRange Gaming

"CyberRange Gaming"
SENTINEL implementation paths ➢ Sentinel Dashboard Menu -> Cybersecurity -> CyberRange

3.6 Pilot Evaluation Results

FFV questionnaire-based evaluation has been filled. To support and complement the FFV Validation activities, CG provide a more descriptive report and extensive comments from their experience of FFV testing by filling a “Data Sheet Report” for a detailed description of UI and UX issues that has been discovered. Comments were made upon the Sentinel content, the results in GDPR and PDP context as well as on UI and UX.

To receive feedback from CG end-users, who conducted operational trials to test the FFV functionalities upon specific experimentation, two online questionnaires of the SENTINEL main functionalities[1] and the CyberRange Gaming external simulation environment[2] were dispensable, as explained in Section 3.5.1, addressing both technical and non-technical evaluation aspects. The 2 questionnaires content is similar to the content of the consolidated version of the User Evaluation Questionnaire presented in Appendix-I.

Overall, the CG end-users responded to a set of questions categorized into the following sections:

- User details
- User Satisfaction
- UI/UX
- CyberRange Gaming
- Security and Results Quality, Personal Data Protection and Compliance
- Business Performance
- Express user’s opinion and additional comments

The questionnaire was answered either via textual justification or through multiple choice, selection or by indicating preferences via a 6-degree Likert scale from 1 (not applicable) to 6 (strongly agree):

- 1 (not applicable)
- 2 (strongly disagree)
- 3 (disagree)
- 4 (neither agree nor disagree)
- 5 (agree)
- 6 (strongly agree)

[1] https://forms.gle/RF67ShiP2fq1G4q39
[2] https://docs.google.com/forms/d/e/1FAIpQLSe9kwBBDDH1AeM3vTEW4oGvfuNNDhyEmZTP46vHNvlRB-gU-g/viewform?usp=sf_link

The analytics of the evaluation results derived from the questionnaires were elaborated and presented in a quantitative approach. To this end, histograms and pie charts were developed which are indicatively depicted in the following description.

3.6.1 User Details

The two respondents from CG organization are from the IT department, one being a software engineer while the other one a developer both having an intermediate level of cybersecurity and GDPR expertise. In addition, they are involved in performing cybersecurity, privacy or personal data protection processes and they employ open-source tools for privacy assessment to estimate and/or support GDPR compliance in their organization. These participants believe that the SENTINEL platform can help them to solve the following two problems:

- Achieve GDPR compliance in everyday procedures.
- Patch management.
- Keeping everyone updated with the Laws and the EU regulations.
- Point out cybersecurity flaws and GDPR noncompliance and suggest possible improvements.

3.6.2 User Satisfaction

Concerning the SENTINEL platform *learning/usability capacities*:

- Both respondents agreed that the *"Creation of their organisation profile"* and "Acquiring policy recommendations" is easy to understand and accomplish compared to **GDPR CSA, DPIA and CSRA** components. Furthermore, one of the respondents agrees that the **Policy monitoring** and **Browsing the Observatory** are also easy to understand and accomplish in the SENTINEL platform.
- Both respondents agreed it was easy to understand the structure and logic of the SENTINEL Dashboard Menu and easy to use.
- Both respondents show almost 100 % satisfaction regarding the performance of the SENTINEL system in terms of speed.
- One of the end users finds that the SENTINEL recommendations for undertaking technical and organisational measures to increase their level of security and GDPR compliance are described accurately and clearly, whereas the other participant neither agree nor disagree on this.
- Concerning performance efficiency and time behaviour, the respondents require more than 60 mins to complete each experiment workflow.

3.6.3 User Interface/User Experience (UI/UX)

- Both respondents agreed or strongly agreed that:
    - The characters on the screens are easy to read.
    - SENTINEL has clearly marked way-finding buttons.

  - the use of terms throughout SENTINEL is consistent.
  - the position of messages on the screens is proper.
  - The different screens of SENTINEL are cohesive in look-and-feel.

- Furthermore, the respondents agreed that SENTINEL provides all the functions and capabilities they expect to have for validating organisation's personal data Processing Activities.
- Finally, respondents seem do not have a strong opinion on the language used and the information (i.e., on-screen messages, and other documentation and tooltips) provided within the dashboard thus they select neither agree nor disagree on the questions related to comprehensiveness of the language and clearness of the information provided with the SENTINEL dashboard.

3.6.4 CyberRange Gaming

This section captures questionnaire's responses concerning the CyberRange Gaming environment of SENTINEL. The respondents agreed that:

- the CyberRange Gaming environment a realistic environment in emulating real-world cyber threats and incidents.
- the CyberRange Gaming environment helps to detect, analyse and better understand vulnerabilities on ICT infrastructure assets.

Furthermore, a respondent commented:

- "Playing with the CyberRange was not a gaming experience but a good test of my knowledge. It needs homogenisation in the interface in terms of vocabulary".
- "The test was not easy for a normal web/office user, but it covered a big range in many issues of daily office /web procedures. It needs to be more interactive and I would prefer to have a more "come back" architecture (like to play again and again)".

3.6.5 Security and Results Quality, Personal Data Protection and Compliance

Both respondents agree that SENTINEL measures can

- Increase GDPR compliance of the experiment's processing activity in an efficient manner.
- can assure privacy of related data.

Furthermore, one of the end users found useful recommendations and suggested tools related to anonymisation and pseudonymization related to their experiment.

Both respondents successfully performed SENTINEL Cybersecurity Risk assessment and identified risks/threats to their registered assets. On the contrary, they find it difficult to identify possible attack scenarios via the SENTINEL Cybersecurity simulation environment.

Both end users think that SENTINEL measures and recommendations can mitigate risks/threats identified within their experiments.

3.6.6 Business Performance

The respondents agreed the following:

- SENTINEL services can help address challenges they face in their organisation with respect to privacy and cybersecurity.
- SENTINEL can be used for all processing activities and assets used for data storage and accessibility in their organisation.
- The measures recommended by SENTINEL will improve the effectiveness of their organisation regarding cybersecurity and personal data protection processes completion.

Furthermore, the measures recommended by SENTINEL can improve

- PII during the submission process.
- Cybersecurity protection of all stored data.
- Implementation of controls that limit any type of unauthorized access to the data.

Finally, respondents seem to not express strong opinion on the “easy-to-learn” aspect of the SENTINEL platform. Furthermore, they were not sure whether they would use additional human and/or financial resources (other than SENTINEL) to implement the suggested measures.

3.6.7 Express user’s opinion and additional comments

The current part of the SENTINEL end-user Evaluation questionnaire illustrates additional feedback and comments provided by the respondents. For the quality of SENTINEL assessment results one of the end users stated that “Although recommendations provided can improve GDPR Compliance and Data Protection, a stronger connection between the assessments and recommendations would be beneficial in order to better understand the results, what actions are critical and how to prioritize them”. While the other one stated “SENTINEL is better than my expectations as a data controller. Missing option as a processor”.

For the quality of the SENTINEL cybersecurity risk assessments one of the respondents elaborated that the “Cybersecurity results are useful for highlighting that additional actions are needed in order to secure the system, but cannot replace the security procedures i.e., penetration testing, needed to actually make the system secure”.

Furthermore, one of the end users found that the “GDPR Compliance and Data Protection recommendations” while the other respondent “fast reports/results” as the most positive aspects concerning the functionalities of the SENTINEL FFV.

Concerning the identification of potential issues (e.g., bugs, content, layout, design, errors, etc.) the respondents faced while using the platform to test the functionalities of the SENTINEL FFV, the respondents mentioned:

- “Register time interval to confirm the email is too short (5min)”.
- “During PA form I lost my input even if I press save as a draft”.

- “Some drop down menus, especially on software versions are not shorted making it unusable filling for the first time might be time consuming”.
- “I miss-filled a question and I could reset it (clear the answer)”.

Finally, based on their company needs, they described any additional services/capabilities that they would like to see in the next versions of the SENTINEL platform:

- “More interactivity, more flexible interface to keep me login again and again”.
- “A stronger connection between the assessments and recommendations i.e., visualizing which of the recommended actions are critical in order to improve the specific categories shown in the assessment tab”.

3.6.8 Additional Feedback collected from pilot end-users

Apart from the validation results received from the questionnaires, described in Sections 3.6.1-3.6.7, the CG pilot end-users have also provided additional feedback to further address any remaining critical technical issues of the SENTINEL FFV platform. This additional feedback has been classified per use cases, priority and type. In some cases, the end-users have also provided suggestions which could be further considered in technical implementation activities. These lists of received feedback are presented in the following tables.

Table 14. SENTINEL pilot users feedback provided for platform registration process and dashboard

Feedback description	Priority	Type	Suggestions
Platform registration process			
Email Verification: Email Verification in 5 min is very short	1 Low	Usability	Need to be at least active for one day 24 hours.
Organization Verification: Should not be checking email	1 Low	Functionality	Maybe a code you give to the organization when they become users. It is safer and not all companies have corporate mails.
Dashboard			
Menu arrows: does not work well	1 Low	Functionality	should shrink Menu and leave only the icons.
Subtitle: "shop" is not the proper word	1 Low	Usability	assistant would be better
User: Active username should be visible in the page under the user icon username must be visible	3 High	Usability	-
Notification Bell: There is no sign that there are notifications	2 Medium	Usability	Bell must be red

Notifications: Should be in the Dashboard main page	2 Medium	Usability	Notifications and actions must be in central post in the dashboard
Notifications: Events are not user friendly and seems irrelevant	2 Medium	Usability	Alt text must be visible as description
UI layout: on low resolutions top right button has strange behaviour	2 Medium	Usability	-
Log out: not user-friendly page. Look like an error page.	2 Medium	Usability	More friendly interface to login page

Table 15. SENTINEL pilot end-users feedback provided for My Organisation

Feedback description	Priority		Type	Suggestions
My organisation				
My organisation - Progress bar: should be green when is 100%	1 Low		Usability	-
My organisation - Help: there is no need for inline help in this page	1 Low		Functionality	remove the question marks.
My organisation - Edit button: does not press on click	1 Low		Functionality	need a small animation
My organisation - Title: mouse over act like a link without linking to any page	1 Low		Functionality	remove mouseover behaviour
My organisation - Edit: Top section is missing	2 Medium		Usability	show edit to a modal popup or add the top section
My organisation - Sector: "other" - need a free text	2 Medium		Usability	-
My organisation - Country: "other" - need a free text	2 Medium		Usability	-
My organisation - Size: comma in options means AND or OR	2 Medium		Usability	-
My organisation – contact- table titles: help is not necessary in all the tabs	1 Low		Usability	-
My organisation-contact-table titles: tooltip on PAs is not Correct (it is the	1 Low		Functionality	-

number not the short name)				
My Organisation-Assets Inventory - Edit page title: edit page has wrong title ("Add asset")	1 Low		Functionality	change title to edit asset
My Organisation-Assets Inventory - Edit page: fields data are not loaded	2 Medium		Functionality	need a field loader or a page loader
My Organisation-Assets Inventory - Edit page: fields data are not shorted, cannot find my version	3 High		Functionality	need to be shorted
My Organisation – GDPR: Is not very clear what to do in this page	2 Medium		Usability	-
My Organisation – OTMs: Is not very clear what to do in this page	2 Medium		Usability	-
My Organisation – OTMs: I face a problem when I try to select an option. It returns to GDPR page. I had to log out and login again to work again	3 High		Functionality	-

Table 16. SENTINEL pilot end-users feedback provided for Processing Activities

Feedback description	Priority	Type	Suggestions
Processing Activities			
Master Page: data number is not correct when other is selected	1 Low	Usability	Instead of the number show the fields ("Other" does not mean nothing on its own).
Edit: I can edit other users' PA	1 Low	Functionality	-
Edit: To change a field, I have to go through all pages with next	3 High	Usability	-
Edit: Details is required but tooltip text says optional	1 Low	Usability	-
Edit: responsible person must be free. I might need to put someone who is not registered	2 Medium	Functionality	-
Edit: Optional drop-down fields do not have a way to empty the field when you select an option	2 Medium	Functionality	-
Edit: Data categories there is a star in the field	1 Low	Usability	-
Edit: Retention period (months), we keep data less than a week	1 Low	Usability	Better explanation and validation or a dropdown with numbers

Edit: Help"?" is not active in many fields	1 Low	Usability	-
Edit: Add a new asset -> Cyber footprint-> has loading and sorting problems	1 Low	Functionality	-

Table 17. SENTINEL pilot end-users feedback provided for Cybersecurity, Policy and Observatory

Feedback description	Priority	Type	Suggestions
Cybersecurity, Policy, Observatory			
Simulation Environment: Is not very easy to complete the fields.	2 Medium	Usability	Need loading animation and sort data
Recommendations: It is not easy to find the where the current recommendations are	2 Medium	Functionality	A report in printed format would be even better
Recommendations: training material is huge.	1 Low	Usability	maybe we need a smaller selection to be presented
Observatory: it refers to professional CS and DP experts	1 Low	Usability	-

4. Pilot 2: Tristone Investment Group (TIG Pilot)

TIG Pilot was accomplished by Dimensions Care (DC), a provider of residential care for children as part of Tristone Group. In the following sections 4.1 - 4.5 the objectives, pilot overview, the experiments' goal and workflow as well as the pilot preparation procedures, the workshop for the SENTINEL demonstration to the DC end-users and evaluation results are described. Furthermore, in the context of the TIG Pilot engagements, 2 additional SMEs were invited and accepted to test SENTINEL functionalities upon a generic experiment. The pilot operations, workshop arranged for raising their awareness on SENTINEL, the experiment's details and the evaluation results are described in section 4.7.

4.1 Pilot Objective

DC is an SME based in England's West Midlands. It provides residential care for children aged up to 18-chronological years. It is regulated under the conditions of the Care Standards Act 2000[3] and the resulting Children's Homes (England) Regulations 2015[4]. The regulations are clear that the 'privacy of children is appropriately protected' and Schedules 3[5] and 4[6] prescribe the information that must be processed and retained to ensure compliance. One of the main objectives of this pilot is to use the SENTINEL platform and assess the privacy and security of "Dimensions Care Children" and "Security of Dimensions Care staff recruitment data" packages and further improve their security, retention, and maintenance via SENTINEL OTMs.

4.2 Pilot Overview

The DC pilot case refers to ensuring effective risk management processes, robust systems of governance and compliance with regulation and high standards of practice. The following table provides an overview of the DC pilot case.

Table 18. DC pilot case

Case overview	**To ensure quality social care services and safeguard vulnerable people.**
Case company	DIMENSIONS CARE LIMITED https://dimensionscare.com
Business context	Dimensions Care provides a bespoke model of residential care for vulnerable children aged up to the age of 18, encompassing a unique model of therapeutic intervention. The children placed with Dimensions Care will have previously experienced trauma, a profound sense of rejection, neglect, abuse, and exploitation. Children in Dimensions Care placements will have been either (a) removed from their biological parents due to harm or abuse, or (b) placed in a children's home with the agreement of the parent due to concerns about parental capacity to meet the needs of a child and prevent harm.

[3] Care Standards Act 2000
[4] Children's Homes (England) Regulations 2015
[5] Scedule3
[6] Scedule4

Provided solution	Collection of processes and information storage of highly sensitive data and information. Depending on the circumstances, this must be shared with designated employees (only) of commissioning authorities, regulators (sector-specific) and auditors, as well as appropriate colleagues.
Current capabilities	The flow of information is administered from administrational centres (i.e., offices) and individual children's homes (i.e., "settings"). It is the responsibility of the manager of each setting (N.B. the Registered Manager (RM)) and the Responsible Individual (RI)[7] to ensure that relevant and lawful data protection principles are maintained. The systems and processes used to manage data are broad and subject to clearly defined principles of conduct. The conduct of colleagues is set through policy and augmented through induction processes, confidentiality agreements, training, supervision, and managerial oversight.
Type of Data	• **Financial and operational data** streams include detailed income and costings, occupancy data, as well as qualitative and quantitative data for service quality assurance and regulatory compliance (for example). • **Social Care Data** of children in Dimensions Care is an essential part of day-to-day practice. The data and information held by the organisation builds up a profile of each child in placement and tracks measurable progress, individual feedback, incidents and events, personal circumstances, and individual histories (for example). Without this information, colleagues cannot meet the welfare and wellbeing needs of the children for whom care is provided. As such, the flow and accuracy of information is a crucial part of the quality of care provided, but that information must be robustly safeguarded from those seeking to directly or indirectly promote harm or abuse to those children. • **Staff Data** is regularly updated and includes sensitive personal information, financial information, identification, Disclosure Barring Service (DBS) reports, visa dates, supervision reviews, time sheets, references, and risk assessments amongst others. All the data and information used is shared on a strict need-to-know basis. For example, only managers and Human Resources (HR) departments will have access to personal and professional data relating to staff. Equally, staff working in an individual setting will only have access to information about children in that specific setting – i.e., not all children for whom care is provided across the organisation. In summary, the types of data collected are varied. These are as follows: • Quantitative (i.e., Discrete & Continuous) • Qualitative (i.e., Binary [limited] & Ordered/Ordinal) • Personal data (i.e., name, email, location data, home address) • Special data (i.e., race/ethnic origin, religious/spiritual beliefs, generic data, biometric [identification purposes], health data) Regulatory requirements determine the following conditions applied to retention. An example of which is as follows (extracted from the Children's Homes (England) Regulations 2015,

[7] The RI is legally responsible for all settings and works with each RM to ensure that all areas of legal and regulatory compliance are maintained to a high standard. The focus is consistently upon the quality of care provided, which includes safeguarding highly sensitive information about each individual child in placement.

	Section 36: **Children's case records** (1) The registered person must maintain records ("case records") for each child which a) include the information and documents listed in Schedule 3 in relation to each child; b) are kept up to date; and c) are signed and dated by the author of each entry. (2) Case records must be kept (a) if the child dies before attaining the age of 18, for 15 years from the date of the child's death; a) in cases not falling within sub-paragraph (a), for 75 years from the child's date of birth; b) securely in the children's home during the period when the child to whom the case records relate is accommodated there; and c) (d) in a secure place after the child has ceased to be accommodated in the home.
Pilot Operation Expectations	To ensure: a) Effective and robust systems of governance and compliance with regulation and high standards of practice. b) Robust and effective risk management processes, of which security is fundamental. c) Outcomes monitoring, analysis, and accountability.

DC has been undertaken two experiments each one engaging a different PA, summarized in the following tables and further presented in Section 4.5.1.

Table 19. 1st experiment overview of DC pilot case

Experiment name	**Security and privacy of Dimensions Care Children Package**
Experiment Description	To ensure: (a) Effective and robust systems of governance and compliance with regulation and high standards of practice. (b) Robust and effective risk management processes, of which security is fundamental. (c) Outcomes monitoring, analysis, and accountability.
SENTINEL platform	All functionalities of SENTINEL components and plugins
Processing Activity (PA)	Dimensions Care Children's Case Records
Experiment's Variables	Business: Service/product quality, Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization, Cost/effect reduction) CS & PDP: (Compliance, Threat Containment, Data Breach Prevention)
Experiment's Goals	To test the efficiency and effectiveness of the SENTINEL framework in the context of TIG Dimensions Care children's home settings.
Logistics *(Participants and type of users)*	Number of participants (individual users): two (2) User roles: Operations Director/DPO, Business Administrator Key assets: CHARMS MIS which is a central software solution that provides several functions relating to the processing and storing of essential information.
Experiment Workflow	Stage One: Set Up Stage two: Implementation
Test cases	All SENTINEL Use cases
KPIsKRs	*KR-1.2: 40% improved compliance efficiency for SMEs/MEs* Reflective variables: Compliance (conformance)

(where applicable)	*KR-1.3: Reduction of compliance – related costs by at least 40%- against benchmarks defined by stakeholders and EU (International) initiatives.* Reflective variables: Cost/effort reduction *KR-1.4: 30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU.* Reflective variables: Service/product quality, Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization) *KR-1.5: Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility.* Reflective variables: Security (Threat Containment, Data Breach Prevention)

Table 20. 2nd experiment overview of DC pilot case

Experiment name	**Security of DimensionsCare staff recruitment data**
Experiment Description	To ensure: (a) Effective and robust systems of governance and compliance with regulation and high standards of practice. (b) Robust and effective risk management processes, of which security is fundamental. (c) Outcomes monitoring, analysis, and accountability.
SENTINEL platform	All functionalities of SENTINEL components and plugins
Processing Activity (PA)	Safe Recruitment and Criminal Record Checks
Experiment's Variables	Business: Service/product quality, Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization, Cost/effect reduction), CS & PDP: (Compliance, Threat Containment, Data Breach Prevention)
Experiment's Goals	To test the efficiency and effectiveness of the SENTINEL framework in the context of DC staff safe recruitment.
Logistics *(Participants and type of users)*	Number of participants (individual users): two (2) User roles: Operations Director/DPO, Business Administrator Key assets: CHARMS MIS which is a central software solution that provides several functions relating to the processing and storing of essential information.
Experiment Workflow	Stage One: Set Up Stage two: Implementation
Test cases	All SENTINEL Use cases
KPIsKRs *(where applicable)*	*KR-1.2: 40% improved compliance efficiency for SMEs/MEs* Reflective variables: Compliance (conformance) *KR-1.3: Reduction of compliance – related costs by at least 40%- against benchmarks defined by stakeholders and EU (International) initiatives.* Reflective variables: Cost/effort reduction *KR-1.4: 30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU.* Reflective variables: Service/product quality, Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization) *KR-1.5: Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility.* Reflective variables: Security (Threat Containment, Data Breach Prevention)

4.3 Pilot plan and Demonstration setup

Prior to the launch of the FFV testing activities, several preparational activities have been carried out within this pilot case, such as definition of experiments, guidelines and documentation preparation, end-users' recruitment and training completion of Non-Disclosure Agreement (NDA) of a DPIA using a template from the ICO (Information Commissioners Office). To this end, upon DimensionsCare (DC) request, an NDA was signed between its representatives and the SENTINEL project. The NDA template can be found in Appendix-III.

To facilitate the requirements of the Demo Workshop, two DC colleagues were identified for running TIG experiments:

- The Managing Director (MD) who is also the designated Data Protection Officer (DPO) for DC.
- A Business Administrator (BA).

To ensure "real-world" scenarios were promoted it was agreed that the MD and BA would not seek support from DH (TIG) because this could compromise the experience of an SME completing the process. It was agreed that the MD and BA would reach out to relevant SENTINEL technical partners for help and support as required.

Following the same paradigm used in CG piloting activities, the DC end-users were invited to a Demonstration Workshop (M24) to assist them in understanding the SENTINEL FFV and how to test it. The main aim was to bring together DC end-users before inviting them to individual trial sessions, present them the SENTINEL project, its current activities and provide hands-on demonstration on FFV of the SENTINEL platform.

4.4 SENTINEL FFV Demonstration Workshop

The SENTINEL Demo Workshop as part of the 2nd pilot case was conducted on Tuesday 30th May 2023 (M24). More than 15 people attended the workshop. Workshop participants included two (2) DC representatives together with the SENTINEL project partners.

As shown in the workshop agenda (Figure 4) the workshop had a total duration of 2 hours including multiple sections such as a brief introduction to the SENTINEL project, general overview of the workshop scope and main purpose, guidance and clarification of what constitutes a processing activity in relation to the GDPR, security and exploitation risks. There was focused discussion about what constitutes a 'processing activity' as well as hands-on demonstration on the SENTINEL platform and the gaming function. Overall, the workshop was semi-structured, so that the participants were asked questions, but also given sufficient freedom to express their needs in a natural conversation.

	TIG Pilot on Dimensions Care: SENTINEL Demonstration Workshop 30 May 2023 Duration: 12.00-14.00 CET Moderators: FP-ITML	
12.00 – 12.10	Opening & Welcome – SENTINEL Project Overview	**ITML**
12.10 - 12.35	Data Security and Data Protection as enablers for creating value from data	**LIST**
12.35 - 12.50	Tristone HC – Dimensions Care (DC)	**TIG**
12.50 - 13.05	DC Assets, Technologies utilised and data collected / Processing Activities for DC experiment	
13.05 - 13.35	TIG Pilot – SENTINEL Hands-on Training	**INTRA**
13.35 - 13.50	The CyberRange Game	**ACS**
13.50 - 13.40	SENTINEL trial execution and evaluation process: Definitions to TIG pilot end-users on Dimensions Care	**FP, ITML**
13.40 - 14.00	Q&As	**Pilot end-users, SENTINEL partners**

Figure 4. DC pilot: SENTINEL Demonstration workshop agenda

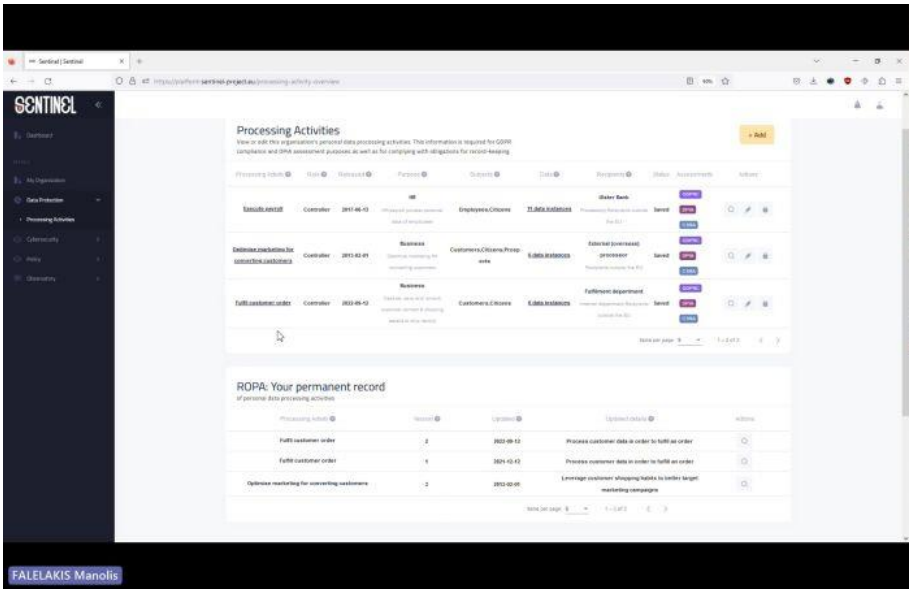


Figure 5. DC pilot: Audiovisual material of the SENTINEL FFV presentation

The main actors of this workshop are presented in the following:

Moderator: the workshop coordinator who initiates the workshop, presented the topics of the agenda and took care of its smooth and timely operation. In addition, the moderator was

responsible for recording the workshop after reaching consensus of all attendees and monitoring the Q&A session.

Project Presenters: the project partners who undertook the responsibility to:

- share knowledge to the workshop participants on topics of GDPR, privacy and data protection.
- present the SENTINEL FFV functionalities and train the participants for the trials' execution.
- provide essential instructions and guidance for the pilot execution and evaluation processes and what must be done to complete the evaluation process.
- record the observations and suggestions.

Participants: DC participants who attended the SENTINEL FFV hands-on training workshop. They presented their company, existing tools/assets relating to the processing and storing of essential information. They were asked to "think aloud" and interact during the workshop sessions and share their thoughts, suggestions etc.

4.5 The SENTINEL FFV Experiment

The following sections describe the purpose and workflow of the experiment the DimensionsCare end-users executed to conduct the SENTINEL trials.

4.5.1 Purpose of the SENTINEL FFV Experiment

The TIG pilot partner engaged two (2) end-users of DC, which is a ChildrenCare SME, as described in Section 4.2. The trials conducted in two sequential rounds, carried out between M25 and M28. During this period, the two end-users (cf. Section 4.2), validated the SENTINEL platform in the context of two (2) focused experiments referring to two (2) SocialCare PAs that DC utilised in their daily normal operations to manage personal data processes.

The purpose of conducting the trials via these two (2) experiments was to engage SME end-users to try and validate the FFV of the SENTINEL platform from the twofold perspective:

- to test and validate the SENTINEL FFV functionalities under real-life operation scenarios and provide feedback considering their personal experience gained after performing the trials considering specific validation criteria, as described in Section 3.5.1.
- to test the way that SENTINEL FFV addresses privacy, personal data protection and cybersecurity requirements of different processing activities performed by DC, a provider of residential care for children (collaborating partner of Tristone).

The two (2) DC end-users executed the trials by running the two (2) pilot experiments using the online SENTINEL platform[8]. To execute the trials, educational and training material was disseminated to the end-users, such as the Demonstration Workshop recording and the SENTINEL End-User instructions for the TIG Pilot end-users (cf. Appendix-II). After completing

[8] https://platform.sentinel-project.eu/

the two rounds of trials in the SENTINEL platform, DC end-users filled out online the User evaluation Questionnaire and the results received are described in Section 4.6.

SENTINEL FFV end-to-end GDPR compliance, privacy and cybersecurity services are thoroughly described in Section 3.5.1. Similar to the CG Pilot, the SENTINEL FFV functionalities were tested via a specific experiment workflow that follows a set of sequential steps. The DC end-users were requested to provide information that concern:

- SME's organisational data.
- SME's PAs of personal data (including assets operating).
- SME's privacy and cybersecurity measures implemented.

DimensionsCare processing activities of the current pilot experiments are vitally important as they provide the appropriate material for establishing the necessary GDPR compliance checks and impact/ cybersecurity assessments.

Moreover, SENTINEL FFV offerings were validated via assessing the security and privacy of DC's personal data processing activities related to children's care and staff recruitment and receiving SENTINEL recommendations that can bolster measures in place to protect personal data as well as reduce the potential for cyberattacks. To this aim, the end-user was requested to access the SENTINEL platform and undertake the two (2) pilot experiments that correspond to two (2) PAs performed by DC. The two (2) experiments together with the engaged PAs are summarized in Table 21, and further described in the following section.

Table 21. Dimensions Care processing activities and experiments

Pilot Experiment	Processing Activity (PA)	Experiment's Goal
1st experiment: "Security and privacy of Dimensions Care Children Package"	"Dimensions Care Children Package"	Use the SENTINEL platform to assess the privacy and security of "Dimensions Care Children Package" processing activity. Receive and identify SENTINEL OTMs to improve the security, retention, and maintenance of personal data.
2nd experiment: "Security of Dimensions Care staff recruitment data"	"Safe recruitment and criminal record checks"	Use the SENTINEL platform to assess the privacy and security of the "Safe recruitment and criminal record checks" processing activity, receive and explore recommendations to bolster the security and privacy of staff recruitment data.

A brief description of the two engaged PAs is provided in the following:

Dimensions Care Children Package. DC is a provider of residential care for children who realizes the processing activity of "Dimensions Care Children Package". The current activity is related to children's residential care. Specifically, children placed in the home(s) are subject to clearly defined regulatory requirements (as confirmed within Schedule 3 of the CHR). These include personal details in relation to the child. Such information must be stored securely by DC and updated in a timely way if changes are required. The retention of the above information, stored securely, is a regulatory condition of practice. Data are shared upon a need-to-know basis.

As an overarching imperative, DC remains cognizant of 'The Golden Rules for Information Sharing'.

Safe recruitment and criminal record checks. DC colleagues (staff) are expected to provide a range of supporting information associated with their suitability to work with vulnerable groups. This is known as safe recruitment (including references and reference verification procedures to address a person's suitability for employment, criminal record checks, employment history, educational history, etc.). The Disclosure and Barring Service (DBS) of DC provides criminal record checks, which may include positive traces that will require further scrutiny in evaluating a person's suitability to work with vulnerable groups.

4.5.2 SENTINEL Use Cases and Experiments Workflow

The two pilot experiments were accomplished by entering the SENTINEL platform and performing a set of SENTINEL use cases.

The SENTINEL use cases rely on four (4) subsequent steps that should be undertaken to utilise the SENTINEL platform functionalities required to execute each of the experiments, as described in Section 3.5.2:

Step 0. Register/Sign in the SENTINEL platform.

Step 1. Utilise the SENTINEL platform to investigate the level of GDPR compliance, privacy, and cybersecurity of the under-examination PA, including its operating assets. Receive a set of tailor-made privacy and security policies and services.

Step 2. Explore policy monitoring services and consult SENTINEL to gather up-to-date information for policy implementation, application of controls and further privacy and security information.

Step 3. Explore the CyberRange Gaming simulation environment for cybersecurity hands-on training.

The SENTINEL use cases to implement these steps, presented in Section 3.5.2 (extensive details are also found in Appendix-II). A short brief is quoted in the following:

- Organisation Profiling
- Completing an assessment workflow
- Acquiring Policy Recommendations
- Policy Monitoring
- Browsing the observatory
- Reporting Incidents
- CyberRange Gaming

4.6 Pilot Evaluation Results

DC end-users tested the SENTINEL platform FFV in two sequential rounds (during M25-M28), as presented in Section 4.5.1. After completing the trials, the end-users filled out the online SENTINEL User Evaluation Questionnaire for TIG Pilot which can be accessed through the following link[9] (a SENTINEL questionnaire template also found in the Appendix-I). The questionnaire entails a set of questions that rely on the sections presented below:

- User details
- User Satisfaction
- UI/UX
- CyberRange Gaming
- Security and Results Quality, Personal Data Protection and Compliance
- Business Performance
- Express user's opinion and additional comments

The two (2) DC end-users answered the online questionnaire either via textual justification or through multiple choice, selection or by selecting preferences via a 6-degree Likert scale from 1 (not applicable) to 6 (strongly agree):

- 1 (not applicable)
- 2 (strongly disagree)
- 3 (disagree)
- 4 (neither agree nor disagree)
- 5 (agree)
- 6 (strongly agree)

The questionnaire results are described in the following sections.

4.6.1 User Details

DC end-user respondents have managerial positions, reside in Head Office and Business Administration departments. Their area of expertise is Health and SocialCare, both considered beginners regarding cybersecurity and privacy. They are currently involved in privacy and personal data protection processes in their organization.

Dimensions Care employ external consultants/services for privacy assessment related to GDPR compliance. Specifically, DC has annual expenses for GDPR compliance maintenance and

[9] https://forms.gle/rBj2EZk4Y9uQenVz8

implementation of OTMs equal to 1,000-9,999 €. DC undertakes compliance audits on an annual basis adopting annual license for GDPR compliance as well.

They both concern lack of knowledge and understanding in cybersecurity. Furthermore, one end-user commented that they are facing some issues with their IT systems and run sporadic phishing and pen tests.

The end-user continued expressing that SENTINEL can help them to expand their knowledge on GDPR and how this aligns with cybersecurity.

4.6.2 User Satisfaction

The current section highlights the responses received by DC end-users applying to user satisfaction, learning and usability questions concerning their experience gained after testing the SENTINEL platform:

- Both respondents agreed that it was easy to understand and accomplish the **DPIA** in the SENTINEL Platform.
- Both respondents were satisfied with the performance of the SENTINEL system in terms of speed when filling out the organisation details. An end-user responded also positively for the speed performance of the SENTINEL system when executing the **GDPR CSA.**
- Both respondents commented that the time required to complete the experiment's workflow was more than 60 minutes.
- Both respondents either strongly agreed or agreed that the SENTINEL platform gave error messages that clearly told them how to fix problems.
- In terms of improving the SENTINEL platform's functionalities, respondents suggested to ameliorate aspects of content, terminology, and wording.

4.6.3 User Interface/ User Experience (UI/UX)

This section provides the end-users' responses related to the UI/UX of the SENTINEL platform:

- Both respondents agreed that the characters on the screens are easy to read.
- Both respondents agreed that the use of terms throughout SENTINEL is consistent. Nevertheless, they supported that the language used in SENTINEL could be improved to be more comprehensive, as commented in the previous section.
- Both respondents replied that the organization of information of the SENTINEL platform, including on-screen messages and their position, and other documentation and tooltips explored via the dashboard menu could be improved.
- Both respondents agreed that SENTINEL has clearly marked way-finding buttons.
- Both respondents agreed that the different screens of SENTINEL are cohesive in look-and-feel.

- Both respondents agreed that the interface of SENTINEL is pleasant.

4.6.4 CyberRange Gaming

With respect to the CyberRange gaming external simulation environment, possibly, due to their low level of expertise in cybersecurity, the end-users faced some difficulties in understanding and testing the CyberRange Gaming, specifically in:

- exploring different types of threats and attacks related to data storage and accessibility.
- analysing and understand vulnerabilities on ICT assets.

Moreover, the two (2) end-users commented that they met technical difficulties, such as freezing screens, and that they had to download other browsers to use it.

4.6.5 Security and Results Quality, Personal Data Protection and Compliance

In the following, the DC end-user responses associated with security and quality of results, personal data protection and compliance are presented.

- Concerning SENTINEL **OTMs/ recommendations**:
    - Both respondents agreed that the SENTINEL measures/recommendations increase GDPR compliance of the experiment's Processing Activity in an efficient manner.
    - Both respondents either strongly agreed or agreed that the SENTINEL measures/recommendations can assure privacy of related data.
    - Both respondents agreed that SENTINEL measures/recommendations can mitigate risks/threats identified within their experiment.
    - Both respondents agreed that privacy incidents can be prevented by implementing SENTINEL recommendations.
- With respect to the **SENTINEL Cybersecurity simulation environment**, both respondents could not easily identify risks/threats to the registered assets. In this context, a respondent expressed that he/she found technical difficulties and continued that if these technical issues didn’t exist, he/she could have gained knowledge on identifying risks via the cybersecurity simulation environment.

4.6.6 Business Performance

The section contains provides DC end-user responses on questions pertaining to business performance:

- Both respondents agreed that the SENTINEL services can help them address challenges they face in their organisation with respect to privacy and cybersecurity
- Both respondents supported that they faced some interruptions while using the SENTINEL platform

- Both respondents agreed that SENTINEL can be utilised for all processing activities and assets used for data storage and accessibility in their organisation.
- Concerning the measures recommended by SENTINEL:
  - Both respondents agreed that they can improve the cybersecurity of all stored data.
  - Both respondents agreed that they can improve implementation of controls that limit any type of unauthorized access to the data.
  - Both respondents agreed that they can improve the security of information/data exchange.
  - Both respondents agreed that SENTINEL measures/recommendations can improve the maintenance and retention of data.
- Both respondents didn't find the SENTINEL platform so easy to learn.
- Both respondents were not satisfied with the time needed to complete **the privacy assessment (GDPR CSA and DPIA)** and receive recommendations.
- Both respondents agreed that the measures recommended by SENTINEL will improve the effectiveness of their organisation regarding cybersecurity and personal data protection processes completion.

4.6.7 Express end-user opinion and additional comments

In this section, the DC end-users provided further feedback and comments regarding the SENTINEL platform:

- Concerning describing in general the quality of **SENTINEL privacy assessments (GDPR CSA and DPIA)** results, the respondents answered that SENTINEL assessments are helpful and in good quality, but they had difficulties in the performance.
- With respect to the quality of **SENTINEL CSRA**, an end-user replied that he/she was satisfied with the risk analysis but didn't find easy to reach the assessment. The other end-user answered that faced freezing screen problems.
- Concerning specifying any issues (e.g., bugs, content, etc.), the end-users faced while utilising the SENTINEL functionalities and testing the platform, an end-user pointed out again errors existence and freezing whilst using platform. The other end-user answered that specifically, the **CyberRange** gaming often froze despite re-entering it and thus, he/she was unable to complete it.
- Both DC end-users described that the most positive aspect of the SENTINEL platform is that it provides insight into the GDPR necessity. In addition, an end-user commented that, SENTINEL has clear dashboard layout and easy-to-follow navigation.
- Regarding additional services/capabilities that they would like to see in the SENTINEL platform, according to their specific requirements, both end-users commented on clearer terminology and the use of **CyberRange** simulation environment without faults.

- The DC end-users provided further comments/suggestions for improvements after experiencing SENTINEL. In this regard, both end-users answered that SENTINEL needs to be more user-friendly and continued that CyberRange gaming depicted in French as default language and that this should be changed into appropriate (English) language, as they find difficult to figure out how to select the other language. Eventually, an end-user commented that SENTINEL is "*an overarching platform"* that can be "*compatible with all the online services*" they currently use, store, and protect with "*clear guidance*" consulting whether their activities are in line with necessary laws and legislation.

4.7 Additional TIG pilot testing and evaluation activities

TIG pilot owners seek to reach out to SMEs within the TIG group to ascertain business leaders' willingness to engage with TIG pilot activities. As shown below, three (3) additional businesses expressed an interest in participating in the activities:

- Beyond Limits
- Next Steps
- Sportfit Support Services ("Sportfit")

Following an initial expression of interest, "Next Steps" were unable to continue with the piloting activity due to operational constraints.

It is worth mentioning, that the SMEs identified come under the umbrella of Health and Social Care of TIG. Specifically:

- Beyond Limits provides support in the community for adults with mental health difficulties and learning disabilities.
- Sportfit have a children's home, operating under the same conditions as the Dimensions Care pilot organisation. However, Sportfit provides semi-independent supported accommodation to young people leaving care. This means providing young people with targeted support in the community to enable independence in adult life.

4.7.1 Objective and Overview

The main objective of engaging these two (2) SMEs (Beyond Limits & Sportfit), as part of TIG pilot case, was to test and validate SENTINEL FFV functionalities upon a generic experiment which encompasses a personal data processing activity utilised in SMEs' daily normal operations. An overview of the generic experiment undertaken for Beyond Limits & Sportfit is presented below in Table 22:

Table 22. Overview of TIG Pilot experiment on Beyond Limits and Sportfit

Experiment name	Generic experiment
Experiment Description	Generic experiment involving employee and prospect data.
SENTINEL platform	All SENTINEL functionalities

Processing Activity(s)	2 PAs: i) Recruitment Process, ii) Marketing activities and communications
Experiment Variables	Business: Service/product quality, Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization, Cost/effect reduction) cs & pdp: (Compliance, Threat Containment, Data Breach Prevention)
Experiment Goal	To test the efficiency and effectiveness of the SENTINEL framework in the context of TIG Beyond Limits and Sportfit privacy and cybersecurity.
Logistics *(Participants and type of users)*	Number of participants: two (2) end-users User roles: Head of Compliance, Finance Director
Experiment Workflow	Stage One: Set Up Stage two: Implementation
Test cases	All SENTINEL Use cases
KPIsKRs *(where applicable)*	*KR-1.2: 40% improved compliance efficiency for SMEs/MEs* Reflective variables: Compliance (conformance) *KR-1.3: Reduction of compliance – related costs by at least 40%- against benchmarks defined by stakeholders and EU (International) initiatives.* Reflective variables: Cost/effort reduction *KR-1.4: 30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU.* Reflective variables: Service/product quality, Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization) *KR-1.5: Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility.* Reflective variables: Security (Threat Containment, Data Breach Prevention)

4.7.2 Preparation, Demonstration setup and Workshop

All SMEs within the TIG group understand the relevant and continued need to comply with GDPR. Having this in mind, the SENTINEL partners have managed to allocate some time to schedule short pilot activities with two additional SMEs as part of TIG group. This was also beneficial for project validation prospective as engaging the Sportfit and Beyond Limits SMEs additionally could expand the list of the project's potential end-users and increase the impact of SENTINEL testing and validation efforts. As these companies belong to the TIG group, we used the same preparational activities, described in Section 4.3 and directly organised a dedicated Demonstration Workshop in M29 for the two (2) end-users. During this workshop, the SENTINEL partners provided a full introduction and summary orientation of the platform. The workshop was condensed and provided as a bespoke means to inform Beyond Limits and Sportfit of:

- clarification of SENTINEL requirements.
- platform orientation, including the gaming functions.
- agreed dates for completion of the pilot activities.

The SENTINEL partners followed up with written guidance and a firm offer of continued support, as required.

4.7.3 The SENTINEL FFV Experiment

The purpose and workflow of the SENTINEL FFV experiment conducted by the two end-users of Beyond Limits and Sportfit engaged by TIG are presented in the next sections.

4.7.3.1 Purpose of the SENTINEL FFV Experiment

The main purpose of the additional testing and evaluation of Pilot 2, as presented in Section 4.7.1, was to engage more SMEs in the context of TIG group activities (Task 6.2) to test/validate SENTINEL FFV functionalities upon a generic experiment related to personal data processing activity utilised in SMEs' daily normal operations.

To this aim, two (2) end-users conducted trials and evaluated the SENTINEL platform coming from two (2) different companies from Socialcare, one related to supporting vulnerable adults in their homes (within the community) and one associated with providing accommodation to young people leaving care. Both end-users conducted the trials during M29. The two end-users tested and validated the SENTINEL FFV functionalities towards generic experiments and upon predefined PAs provided by the SENTINEL platform related to managerial and staff recruitment processes. These PAs comprise the use and management of generic personal data with processes that are common to most companies and organisations.

To raise awareness of the SENTINEL platform and its functionalities, the end-users received the workshop recording of the SENTINEL Demonstration they attended and corresponding instructions similar to Appendix-II. After conducting the trials, they completed the questionnaire for these generic experiments.

Each end-user conducted one (1) generic experiment, incorporated a corresponding generic PA, as summarized in Table 23.

Table 23. Processing Activities and Experiments of TIG additionally engaged SMEs

Pilot Experiment	Processing Activity (PA)	Experiment's Goal
1st experiment: Generic experiment with employee data involved	"Marketing activities and communications"	Use the SENTINEL platform to assess the privacy and security of a generic processing activity related to marketing and communication activities. Receive and identify SENTINEL OTMs to improve the security, retention, and maintenance of personal data**.**
2nd experiment: Generic experiment with prospect data involved	"Recruitment Process"	Utilise the SENTINEL platform to assess the privacy and security of a generic processing activity related to staff recruitment procedures. Receive and identify SENTINEL OTMs to improve the security, retention, and maintenance of personal data**.**

The **"Recruitment Process" PA** refers to information gathered to recruit new starters and involved employee data.

The **"Marketing activities and communications" PA** involved prospect data processing of potential customers for marketing purposes.

4.7.3.2 SENTINEL Use Cases and Experiments Workflow

The two end-users were invited to follow a linear pipeline of actions, as presented in the DIH Pilot generic experiment (Section 5.5.2) and thoroughly analysed in Appendix-II, to raise awareness and provide a set of tailor-made recommendations to their organisation:

1. Create a complete profile for your organisation.
2. Create and populate one or more personal data PAs.
3. Commit at least one PA to the ROPA.
4. Execute one or more self-assessments:
    - GDPR CSA
    - DPIA
    - CSRA
5. SENTINEL leverages data gathered during the previous steps, to calculate recommendations of measures, software, and training material, tailored to your organisation. These may be browsed under "Policy".
6. SENTINEL keeps track of which recommended measures are implemented by each organisation, and which measures are still pending.
7. Explore the CyberRange interface, to recreate the cyber setup of your organisation and learn how to do cyber defense. Play around in the new CyberRange gaming interface to discover best cyber defense practices in action.
8. Browse the Observatory for:
    - Up-to-date information on the latest threats and vulnerabilities data from open threat intelligence platforms (for expert and technical cybersecurity staff)
    - Handling incidents and reporting/sharing them to the appropriate communities.
    - Selected and curated content and training material on best practices for cybersecurity and data protection.

4.7.3.3 Evaluation results of additional pilot activities

The two (2) end-users engaged from Sportfit and Beyond Limits, respectively, conducted trials on the SENTINEL platform and evaluated the SENTINEL FFV functionalities within M29. After completing the trials, the end-users filled out the online SENTINEL User Evaluation Questionnaire[10] (presented in cf. Appendix-I as well).

The questionnaire incorporates a group of questions contained in the below sections:

- User details

[10] https://forms.gle/RKsx5Ta3CcBo1TFD7

- User Satisfaction
- UI/UX
- CyberRange Gaming
- Security and Results Quality, Personal Data Protection and Compliance
- Business Performance
- Express user's opinion and additional comments

The two (2) end-users answered the online questionnaire either with textual justification or by selecting options towards multiple choices or by choosing preferences in a 6-degree Likert scale from 1 (not applicable) to 6 (strongly agree):

- 1 (not applicable)
- 2 (strongly disagree)
- 3 (disagree)
- 4 (neither agree nor disagree)
- 5 (agree)
- 6 (strongly agree)

The questionnaire results are provided in the following sections.

4.7.3.3.1 User Details

The first end-user is the Head of the compliance department, whereas the other end-user is Director in the Finance Department. Both end-users have expertise in Health and SocialCare. One of the end-user is a beginner in cybersecurity and privacy, whereas the other end-user has an intermediate level of expertise in cybersecurity and privacy. An end-user is not currently involved in privacy and personal data protection processes in their organization. The other end-user is involved in terms of Arranging Penetration Testing of organisation's systems, updating Policy and Procedures.

Both end-users answered that their organisations do not employ external consultants/services for privacy assessment related to GDPR compliance up to their knowledge, nonetheless, one of them answered that his/her organization plans to invest in such tools/services within the next 2 years (the other end-user replied that no future plans are considered up to his/her knowledge). Specifically, an end-user answered that his/her organization annual expenses for GDPR compliance maintenance and implementation of OTMs are equal to £5000. An end-user responded that his/her organization undertakes annual compliance audits of free and open-source license for GDPR compliance.

An end-user stressed as cybersecurity and privacy concerns in his/her organisation the limited understanding of the legal GDPR framework and/or the scope of potential threats in

Cybersecurity. The other end-user express concern in cyber-attacks. An end-user believes that SENTINEL platform can help his/her organisation to resolve the respective concerns.

4.7.3.3.2 User Satisfaction

Regarding end-users' satisfaction with the SENTINEL platform:

- An end-user found easy to understand the structure and logic of the **SENTINEL Dashboard Menu** and easy to use.
- Both end-users were not satisfied with the performance of the SENTINEL system in terms of speed. An end-user added that the time required to complete the experiment's workflow was more than 60 minutes.

In terms of improving the SENTINEL functionalities, an end-user replied that: "*My assessments don't show under Assessment area on the dashboard"*, "*No error messages if something incorrect the input screen just closed"*, "*first contact entry was duplicated, wasn't able to edit or delete contacts […] it came back later and it worked"*. He/she also added that "*Recommendations are not readily accessible"* and individual selection needed from 10 drop downs. Moreover, replied that *"OTM's do not appear to be specific - same number in red as the generic list"* and that *"Observatory looks aimed at IT professionals rather than beginner or intermediate"*. Furthermore, he/she commented that *"Cybersecurity games were coming up in a mixed language not English as expected"* and overall replied that SENTINEL *"Looks like a useful tool for professionals or consultants engaged solely in Data Protection and Cybersecurity"*.

4.7.3.3.3User Interface/User Experience (UI/UX)

As regards UI/UX of the SENTINEL platform:

- Both respondents agreed that the characters on the screens are easy to read
- Both respondents answered that the language used in SENTINEL could be more comprehensive, nevertheless, an end-user agreed that the use of terms throughout SENTINEL is consistent.
- Both respondents agreed that information (i.e., on-screen messages, and other documentation and tooltips) provided with the dashboard is accurate and clear and one (1) respondent agreed that the organisation of information on the SENTINEL screens is clear and user-friendly.
- An end-user agreed that SENTINEL has clearly marked way-finding buttons (exit, back, next page, etc.
- An end-user agreed that position of messages on the screens is proper.
- An end-user commented that SENTINEL is more helpful for a GDPR professional or consultant who is well versed in data protection laws, whereas further help is needed for non-privacy/cybersecurity professionals to fill out the assessment questions and interpret the recommendations.

4.7.3.3.4 CyberRange Gaming

Regarding the CyberRange Gaming external simulation environment, an end-user faced issues in using it due to the mixed languages. The other end-user didn't test CyberRange Gaming.

4.7.3.3.5 Security and Results Quality, Personal Data Protection and Compliance

The end-users provided the following feedback for the security and quality of results, personal data protection and compliance:

- Concerning SENTINEL **OTMs/ recommendations**:
    - An end-user agreed that the SENTINEL measures/recommendations increase GDPR compliance of the experiment's PA in an efficient manner.
    - An end-user respondent that did not have time to go down the drop lists to read all the information provided for recommendations/suggested tools/techniques that can be utilised to increase the security and privacy of PAs. In addition, he/she suggested that it will be helpful to have a summary of the produced information indicated with red, amber, green scales.
    - An end-user commented that he/she "*found hard to understand the recommendations"*, and that a more experienced person in GDPR terminology needed to apply this to the organisation.
- With respect to the **SENTINEL Cybersecurity simulation environment,** an end-user replied that could not identify risks/threats or possible attack scenarios to the registered asset because of his/her lack of expertise.

4.7.3.3.6 Business Performance

In this section no comments received by the two end-users.

4.7.3.3.7 Express end-user opinion and additional comments

The feedback provided by the two end-users in this section is presented in the following:

- Concerning the quality of SENTINEL privacy and cybersecurity assessments (GDPR CSA, DPIA, CRA) results, an end-user answered that SENTINEL is a useful tool for GDPR Professionals.
- With respect to issues (e.g., bugs, content, layout, design, errors, etc.) the end-users faced while using the platform to test the functionalities of the SENTINEL platform, a respondent replied that the screen at first was jumping about, closing when trying to add, edit and delete contacts, but eventually it was fixed.
- As a general comment for improving SENTINEL, an end-user suggested to separate modules for security and GDPR.

5. Pilot 3: SMEs/MEs engaged via DIH (DIH Pilot)

The following sections present the DIH pilot plan, its main objectives and the content of the pilot use cases and experiments that have been revised and refined according to what has been described in D6.1.

5.1 Pilot Objective

In the frame of the SENTINEL DIH pilot, external SMEs/MEs have been engaged via Digital Innovation Hubs (DIHs), under Tak 6.3 activities, to test and validate the SENTINEL offerings in terms of a generic experiment which addresses all SENTINEL FFV use-cases.

This objective is directly linked with KR- 5.3 “More than twenty (20) entities (e.g. academics and enterprises) to use SENTINEL offerings”, KR-5.4 “More than (8) DIH engaged to further communicate and support SENTINEL offerings”, and KR-6.3 “At least six (6) third-party collaborations to be established for further applicability verification”. Therefore, the DIH pilot aimed at verifying the applicability of SENTINEL offerings to different domain areas, companies with various sizes, business models, legal scope and geographical location.

By collaborating with DIHs, SENTINEL tapped into a vast network of SMEs across various sectors and regions, ensuring that its platform was tested, validated, and optimized for a diverse range of real-world applications. This engagement not only aided in the development of a more inclusive and representative platform, but was also aligned with SENTINEL's goal of democratizing access to high-end digital security tools for all businesses, regardless of their size or financial capabilities.

Moreover, the collaboration with different DIHs has offered strategic advantages in terms of localized market insights, credibility, and resource optimization. DIHs possess a deep understanding of the specific challenges and needs of SMEs in different European regions, including compliance with local regulations and business practices. This knowledge is invaluable for tailoring the SENTINEL platform to meet these varied requirements effectively. Through this collaborative approach, we aimed at fostering a more secure and compliant digital ecosystem for SMEs across Europe, aligning with broader objectives of enhancing digital innovation and cybersecurity readiness at a continental scale.

5.2 Pilot Overview

This section provides a brief overview of the DIH Pilot.

Table 24. DIH Pilot case on external SMEs

Case overview	SMEs/MEs engaged via Digital Innovation Hubs and incubators
Case company	Different DIHs and incubators (Produtech, innova4tech, connect5, innovtourism, Smart Islands Hub, Defense4Tech Hub, Digital Manufacturing Innovation Hub Wales, DIH4CPS, DIH-World)
Business context	Manufacturing, Utilities, Retail, IT, Food Industry, Media, Engineering and Management, Research, Educational, Cybersecurity

Provided solution	SMEs have different core competences. Solutions to be addressed are supported by different technologies such as: CPS, 5G, cloud systems, IoT, Big Data, AI, HPC
Current capabilities	The level of maturity of the SMEs/MEs to be engaged with regards to GDPR and PDP compliance and cybersecurity solutions, will typically vary.
Type of Data	Financial, Operational, HR, Suppliers, IT
DIH Pilot Operation Expectations	To ensure that SENTINEL offerings meet the following expectations: • Reduction of compliance related costs • Improve compliance efficiency. • Protection of sensitive data against different types of threats and attacks. • Reduction in complexity in managing GDP and PDP compliance. • User-friendly solution

Table 25. DIH Pilot Experiment overview

Experiment name	**SMEs/MEs engaged via Digital Innovation Hubs and incubators**
Experiment Description	To ensure that SENTINEL offerings meet the following expectations: • Reduction of compliance related costs • Improve compliance efficiency. • Protection of sensitive data against different types of threats and attacks. • Reduction in complexity in managing GDP and PDP compliance. • User-friendly solution
SENTINEL platform	All functionalities of SENTINEL components and plugins
Processing Activity (PA)	• Staff management and payroll administration • Access to/consultation of a contacts database containing personal data • Sending emails • Fleet management • Website operation • CRM • others
Experiment's Variables	Business: Service/product quality, Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization, Cost/effect reduction) cs & pdp: Compliance (Conformance), Security (Threat Containment, Data Breach Prevention)
Experiment's Goals	To evaluate user experience of SENTINEL in different contexts
Logistics *(Participants and type of users/Pilot Duration/Pilot Location/Others)*	Number of individuals (10) DPO 1 Consultancy 1 IT / Information Security 2 Technology and Engineering 5 Other 1
Experiment Workflow	Stage One: Set Up Stage two: Implementation
Test cases	All SENTINEL Use cases
KPIsKRs	*KR-1.2: 40% improved compliance efficiency for SMEs/MEs*

(where applicable)	Reflective variables: Compliance (conformance) *KR-1.3: Reduction of compliance – related costs by at least 40%- against benchmarks defined by stakeholders and EU (International) initiatives.* Reflective variables: Cost/effort reduction *KR-1.4: 30% increase in the acceptance of intelligent one-stop-shop solutions for compliance services by SMEs/MEs all over EU.* Reflective variables: Service/product quality, Satisfaction (Learnability), Usability, Performance Efficiency (Time efficiency, Resource utilization) *KR-1.5: Protect a real-life SME environment from at least (10) types of related threats and attacks to data storage and accessibility* Reflective variables: Security (Threat Containment, Data Breach Prevention)

5.3 Pilot plan and Demonstration setup

The pilot preparation activities were launched in M19, including DIH engagement, SMEs recruitment, informative and compelling materials creation.

The recruiting phase has started from day zero. However, after the SENTINEL FFV release (M30), additional efforts have been put in place to recruit volunteer SMEs/MEs to test and validate the SENTINEL offerings. During the recruitment phase, the plan was to involve DPOs, software vendors, accounting staff, IT people, and area managers.

Through DIH Pilot activities, SENTINEL continuously evaluates the effectiveness of the engagement strategy and adjusts as necessary. The objective is to provide updates about the progress and insights gained from SME engagement.

Since SENTINEL deals with security and data protection, we ensure that all engagements with SMEs, comply with relevant regulations like GDPR and ethical standards.

5.3.1 SMEs/MEs recruitment

The recruiting process of SMEs was performed through our collaboration with different DIHs. DIHs are well-positioned to identify and engage relevant SMEs due to their regional presence and sector-specific knowledge. The recruitment process involved the creation of informative and compelling materials that explain the value proposition of the SENTINEL platform for SMEs. This included clear information on security, privacy, and data protection features which are the core of the SENTINEL project.

Part of SENTINEL outreach strategy, we've used social media and webinars to leverage the communication channels of DIHs to amplify our main message. In this regard, SENTINEL has hosted webinars in collaboration with DIHs to inform SMEs about the SENTINEL project, its benefits, and the process of participating in platform testing.

5.3.2 Communication

The communication to promote the event was mainly addressed by social media, e-mails, and DIHs' communication channels. The objective of the communication was to engage SMEs through DIH offering solutions for their potential problems with Data Protection and GDPR. The event organized, named SHIELDS Workshop had an online form to capture registration and

collect contact information from SMEs. In total 36 SMEs have registered to the event. We collected the email, name, companies' names, and the authorization for use of data.

Figure 6. SHIELDS workshop posters

The SHIELDS workshop (SENTINEL FFV Demonstration Workshop) triggered the testing and validation phase of SENTINEL platform thought external SMEs. The testing and validation of the platform was a crucial step SENTINEL, but also for SMEs, to ensure that they are effectively safeguarding their data and complying with GDPR regulations.

5.4 SENTINEL FFV Demonstration Workshop

SENTINEL FFV Demonstration Workshop for the DIH Pilot was organized by UNINOVA and ITML on September 25th 2023, which accounted for the participation of 24 SMEs (see Table 26) and 48 attendees in total, including the active participation of the consortium partners. The total duration of the workshop was 2h30 and followed the proposed order.

The complete agenda and a screen of the workshop are depicted in Figure 7 and Figure 8, whereas the participation list is displayed in Table 26.

	SHIELDS Workshop 25 September 2023 Duration: 10.00-12.30 CET Moderators: ITML-FP	
10.00 - 10.05	Opening & Welcome	**UNINOVA – FP**
10.05 - 10.15	SENTINEL Project Overview	**ITML**
10.15 - 10.50	Participants Introduction - Open Survey: PART I	**Attendees – UNINOVA**
10.50 - 11.10 **11.10 - 11.15**	Data Security and Data Protection as enablers for creating value from data Open Survey: PART II	**LIST** **Attendees – UNINOVA**
11.15 - 11.45 **11.45 - 11.55** **11.55 - 12.10**	SENTINEL Hands-on Training CyberRange Gaming Open Survey: PART III	**IDIR** **ACS** **Attendees – UNINOVA**
12.10 - 12.15	Definitions for SENTINEL trial execution and evaluation process	**FP**
12.15 - 12.30	Wrap up – Q&As	**Attendees – SENTINEL partners**

Figure 7. SENTINEL FFV Demonstration workshop agenda

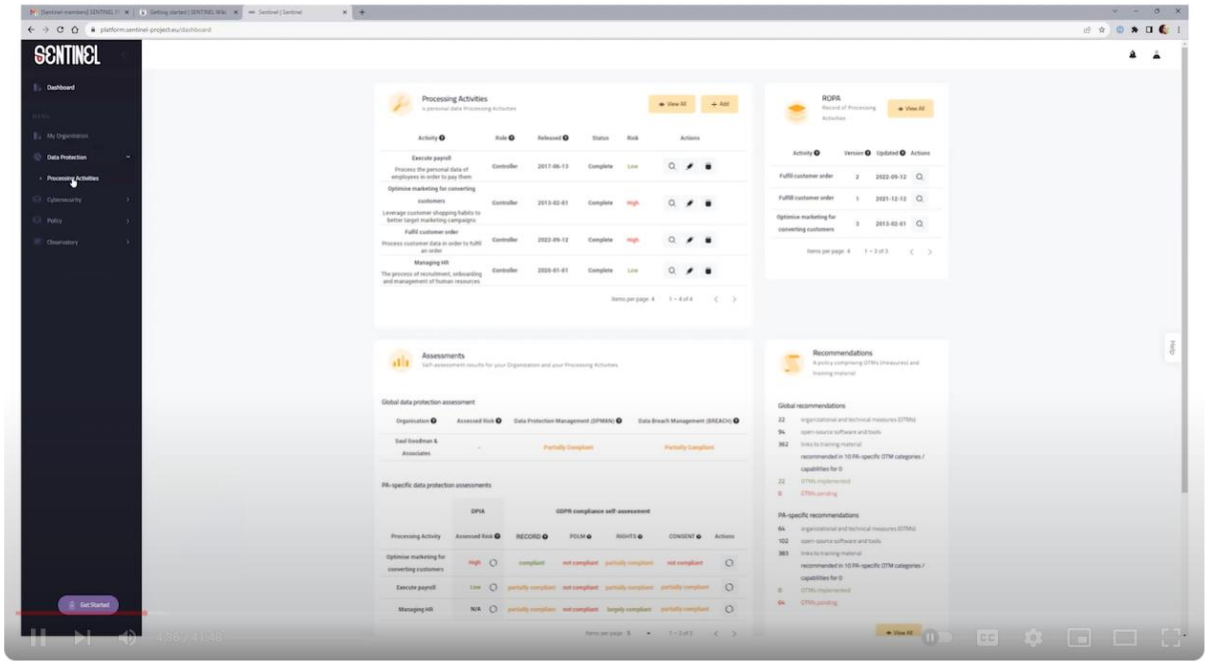


Figure 8. Indicative screen from the Workshop during the SENTINEL FFV demonstration

Table 26. External SMEs workshop participation list

Company:	WebSite	Sector	Short Description
A Ver o Mundo Passar	www.superfm.com	Media	Portuguese Radio Management, Streaming and Multimedia Producer
Analítica	www.analitica.pt	Engineering - Energy	Certification of electrical installations, technical support for professionals in the sector, carrying out audits of inspections and electricity projects, at the National Association for Certifying Electrical Installations – CERTIEL.
António Abreu Metalomecânica LDA.	www.aametalomecanica.com	Industry	The Portuguese Company Antonio Abreu Metalomecânica is a Metal Industry
Bournemouth Cert (BU-CERT)	www.bounermouth.ac.uk	IT	BU Computer Emergency Response Team (BU-CERT) is the product of the fusion of Bournemouth University's IT Services, the Department of Computing and Informatics and the Department of Psychology.
Caixa Mágica Software	www.caixamagica.pt	IT	Caixa Mágica Software creates technological solutions for its customers.
CONSULGAL	https://consulgal.pt	Engeneer	Consulgal is an integrated group of Engineering and Management services companies with employees worldwide.
DRAXIS ENVIRONMENTAL SA	www.draxis.gr	IT	DRAXIS focuses on developing real life environmental ICT solutions and providing specialized environmental consultation services.
EXOS Solutions	www.exos-solutions.com	Industry	A spin-off born at the Polytechnic University of Valencia to provide consulting services in industrial organization (operations consulting) to our clients.
FUTURA	https://futuranet.eu/	IT	Law and IT - Risk assessment
GreenRoads	https://www.greenroads.ai	IT	Greenroads was set up to reduce the environmental impact of transportation by leveraging AI and big data analytics.
JAVALI	www.javali.pt	IT	Javali is dedicated to technological development and digital communication on web and mobile platforms.
Kaizen Tech SA	www.raizen.tech	IT	Data analisys
Knowledgebiz Consulting	www.knowledgebiz.pt	IT	KBZ commercialize products and services originated from technologies resulting from our research and development and that of our partners
Law and Internet Foundation	www.netlaw.bg	Law	Law and Internet Foundation is a Bulgarian NGO & Research centre which supports and performs applied studies, scientific research, programmes and projects.
Nissatech Innovation Centre	www.nissatech.com	IT	Development of application and advanced IT solutions for boosting innovations in

			dynamic and networked business environments.
PIEP	www.piep.pt	Research	The Centre for Innovation in Polymer Engineering (PIEP) is a private association, with a technological and scientific matrix and a business management model.
PT Mills	www.ptmills.pt	Engeneer	Metalworking experts, Pt Mills Lda.
Raven Cybersecurity	www.ravensec.eu	IT	Raven Cybersecurity is a startup specializing in cybersecurity services.
Tequimaq, Lda.	www.tequimat.pt	Industry	TEQUIMAQ designs, develops and builds all types of equipment for the Industry, namely Chemical and Cork.
Tristone	www.tristone.healthcare	HealthCare	The care division of Tristone Capital – Tristone Healthcare Ltd – is committed to the acquisition and growth of social care companies which have proven business models.
UNIPARTNER	www.unipartner.com	IT	Unipartner is an information technology services company that works with government organizations, financial institutions and commercial enterprises to solve their most demanding IT and business challenges.
University of Porto	www.med.up.pt	Educational	The University of Porto is a Portuguese public university located in the city of Porto and founded on March 22, 1911.
VANGUARDA	www.vanguarda.pt	IT	Global Business Management Consulting
Westcon-Comstor Portugal	www.westconcomstor.com	IT	CyberSecurity Solutions

5.5 The SENTINEL FFV Experiment

The current section describes the purpose and workflow of the DIH Pilot generic experiment.

5.5.1 Purpose of the SENTINEL FFV Experiment

The main purpose of the DIH Pilot trials was to engage external SMEs (as part of the activities of Task 6.3) and allow organisations from different Industries to:

- test and validate the available functionalities of SENTINEL FFV under real-life operation scenarios and provide feedback considering their personal experience gained after performing the trials upon validation criteria, such as usability, performance, user satisfaction, UI, speed, flexibility, quality, efficiency.
- to test the way that SENTINEL FFV addresses privacy, personal data protection and cybersecurity requirements of different processing activities utilised by SMEs in their daily business.

In the context of DIH Pilot, ten (10) end-users deriving from ten (10) different companies were engaged to conduct the SENTINEL FFV trials from M28 to M29. The external SMEs/MEs tested

and validated the SENTINEL FFV functionalities either by utilizing specific Processing Activities (PAs) templates provided by the SENTINEL platform related to marketing and staff recruitment processes that involve generic personal data handling processes, common to most companies and organisations or by specifying in the platform their own organizational PA.

The SMEs who specified their own PAs were able to perform a comprehensive data mapping exercise, involving the understanding what data is collected, how it's processed, who has access to it, and where it's stored. SENTINEL platform facilitated this data inventory process. After conducting the trials, they completed the online SENTINEL User Evaluation Experiment.

By testing, validating, and using SENTINEL platform, SMEs were able to establish a robust framework for safeguarding personal data, complying with regulations, and building trust with their customers and partners. By adopting this approach, SMEs will be able to mitigate risks and demonstrates a commitment to data privacy and security.

During the testing and validation, SENTINEL provided technical and operational support to SMEs, including detailed documentation (cf. Appendix-II), and troubleshooting guides, adopting an iterative improvement approach, where the feedback for SMEs is collected to make iterative improvements to the platform. This will not only enhance the platform, but also demonstrate to SMEs that their input is valued and taken seriously. We established clear channels for SMEs to provide feedback on their experience with the platform, mainly through surveys.

The 10 end-users of the DIH Pilot conducted generic experiments of PAs pre-defined in the SENTINEL platform or PAs developed by the SMEs. Details of the generic experiments and the PAs applied in the context of DIH Pilot trials are presented in the following Table 27.

Table 27. Processing Activities and Experiments of DIH Pilot

Pilot Experiment	Processing Activity (PA)	Experiment's Goal
Generic experiment with prospect data involved	"Marketing activities and communications"	Use the SENTINEL platform to assess the privacy and security of a generic processing activity related to marketing and communication activities. Receive and identify SENTINEL OTMs to improve the security, retention, and maintenance of personal data.
Generic experiment with employee data involved	"Recruitment Process"	Utilise the SENTINEL platform to assess the privacy and security of a generic processing activity related to staff recruitment procedures. Receive and identify SENTINEL OTMs to improve the security, retention, and maintenance of personal data.
Generic experiment with citizens data involved	"Project Data Corpus"	Utilise the SENTINEL platform to assess the privacy and security of a generic processing activity related to the handling of citizens personal data processes. Receive and identify SENTINEL OTMs to improve the security, retention, and maintenance of personal data.
Generic experiment with patient data involved	"Collection of personal data within a research study"	Utilise the SENTINEL platform to assess the privacy and security of a generic processing activity referring to collecting personal data from patients within a research study. Receive and identify SENTINEL OTMs to improve the security, retention, and maintenance of personal data.

Generic experiment with employee data involved	"Executing Payroll"	Utilise the SENTINEL platform to assess the privacy and security of a generic processing activity referring to payroll personal data processes. Receive and identify SENTINEL OTMs to improve the security, retention, and maintenance of personal data**.**

5.5.2 SENTINEL Use Cases and Experiments workflow

The SENTINEL functionalities were tested via performing a pipeline of actions, adjusted to the SENTINEL platform's technical updates existed by that time. It aimed at helping the end-users raise awareness and focused their efforts on what matters most for protecting personal data within their SME, without wasting resources on exploratory activities.

The SENTINEL generic experiment, allowed the end-users to get advised by the **"Help Wizard" of SENTINEL enhanced feature,** found by clicking on the "Help" button appearing in the middle right of each SENTINEL screen Figure 9.

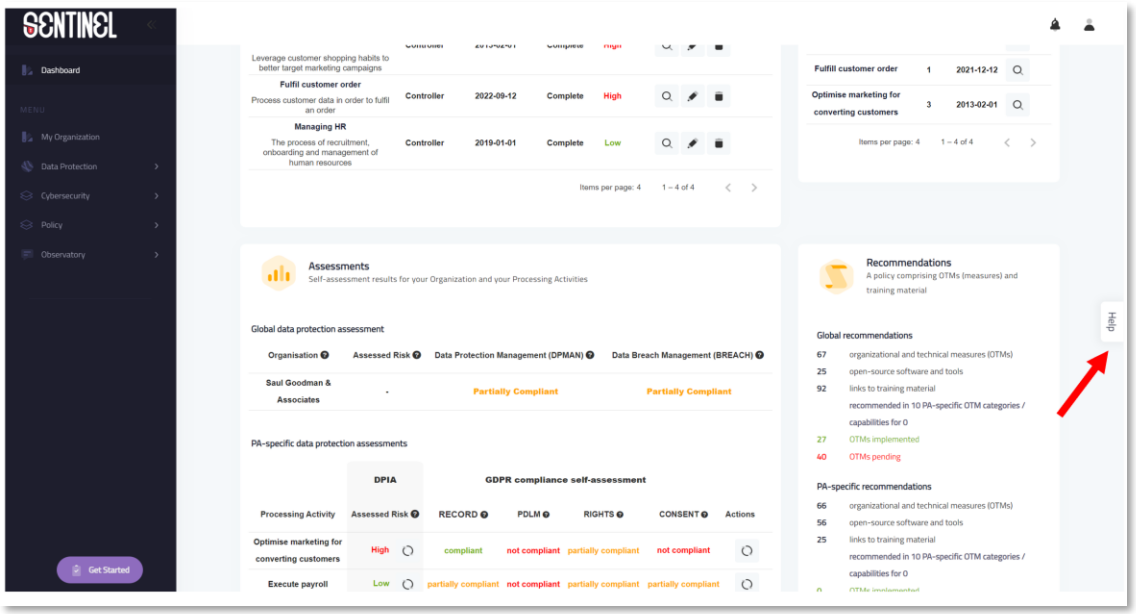


Figure 9. SENTINEL Help menu

In the following, the specific steps for executing the linear pipeline of actions in the SENTINEL platform are briefly presented and thoroughly analysed in Appendix-II.

As an initial step, to utilise the SENTINEL functionalities, the end-user may register/sign in the SENTINEL platform.

0. Register/Sign in the SENTINEL platform

1. Create a complete profile for your organisation

To execute this action, the following items must be filled in the SENTINEL platform sequentially, as shown below:

1.1 Org. Basic data

1.2 Org. Contacts

1.2 Org. Generic assets profile

1.3 Org. Assets inventory

1.4 Org. GDPR compliance

1.5 Org. Measures

2.Create and populate one or more personal data PAs.

Processing Activities (PAs): Information regarding the handling of personal data, represented as a provisional list of PAs and their details. The following capabilities included in creating or populating a PA:

2.1 PAs listing page (Data protection centre)

2.2 Create / edit PA page

2.3 View PA page

3. Commit at least one PA to the ROPA

This action, encompasses the following activities:

3.1 Creating a ROPA entry / committing a PA to the ROPA

3.2 Viewing a ROPA entry

3.3 Exporting a ROPA entry

3.4 Making a PA in the ROPA as inactive

4. Execute one or more self-assessments

The system evaluates the developed organisation profile and especially the registered PA of the experiment and decides whether the organisation is eligible for passing through the **offered assessment workflows** and implements progressively three types of assessments:

4.1 GDPR CSA

4.2 DPIA

4.3 CSRA

5. SENTINEL leverages data gathered during the previous steps, to calculate recommendations of measures, software, and training material, tailored to your organisation

These may be browsed under "Policy". The main purpose of Policy Recommendations is to analyse the organization profile as well as the information registered for each completed PA, and propose human-readable, enforceable, and actionable policy. Considering the full list of proposed recommendations, this section drafts tailor-made optimization policies for your organization regarding its technologies, tools and procedures. The proposed recommendations are grouped in two different groups:

5.1 Global recommendations

5.2 PA-specific recommendations

6. SENTINEL keeps track of which recommended measures are implemented by each organisations, and which measures are still pending

After receiving a set of tailor-made security and privacy policies, the SENTINEL user may track the “implementation status” of the OTMs related to each pilot experiment contained in the policy draft.

7. Explore the CyberRange interface

The SENTINEL CyberRange Airbus gaming interface is an external simulation service for Cybersecurity hands-on training. AIRBUS provides a new training approach with a Gaming interface based on the CyberRange in order to raise awareness. The users learn in an interactive way the best practice to better protect personal and sensitive data. During the trial the end-users saw how to connect to the Gaming interface and start the mission. They learned how to interact with the platform and validate the objectives to fulfill the mission.

Explore the CyberRange interface to recreate the cyber setup of your organisation and learn how to do cyber defense. Play around in the new CyberRange gaming interface to discover best cyber defense practices in action.

8. Explore the Observatory

The user may browse the Observatory to explore:

8.1 Up-to-date information on the latest threats and vulnerabilities data from open threat intelligence platforms (for expert and technical cybersecurity staff)
8.2 Handling incidents and reporting/sharing them to the appropriate communities.

8.3 Selected and curated content and training material on best practices for cybersecurity and data protection.

The user may browse the Observatory either from the “Threat Intelligence” page or from the “Knowledge Base” page as described in the following.

5.6 Pilot evaluation results

In the context of the DIH Pilot activities, as mentioned in Section 5.5.1, ten (10) end-users coming from ten (10) external SMEs, were engaged as part of T6.3 activities and through the SENTINEL FFV Demonstration Workshop (cf. Section 5.4). Two (2) SMEs engaged in the DIH Pilot had participated in the SENTINEL Minimum Viable Product (MVP) testing and validation activities reported in D6.1 [2]. All end-users executed SENTINEL trials following the specific experimentation process and use cases described in Section 5.5.2. They tested SENTINEL FFV functionalities in terms of UI/UX capabilities and according to their privacy, personal data protection and cybersecurity requirements and validated it via filling the online User Evaluation Questionnaire which can be accessed via the following link[11].

The evaluation process carried out in M29, and the analysis of the results conducted within M30 until the composition of the current deliverable. The SENTINEL FFV User Evaluation Questionnaire, incorporates a group of questions supporting the following sections:

- User Details
- User Satisfaction
- UI/UX
- CyberRange Gaming
- Security and Results Quality, Personal Data Protection and Compliance
- Business Performance
- Express end-user opinion and additional comments

The questionnaire was answered either via textual justification or through multiple choice, selection or by indicating preferences via a 6-degree Likert scale from 1 (not applicable) to 6 (strongly agree):

- 1 (not applicable)
- 2 (strongly disagree)
- 3 (disagree)
- 4 (neither agree nor disagree)
- 5 (agree)
- 6 (strongly agree)

The evaluation results derived from the questionnaires were elaborated and analytics data presented in a quantitative approach. In this context, histograms and pie charts were developed which are indicatively depicted per questionnaire category in the following sections.

[11] https://forms.gle/RKsx5Ta3CcBo1TFD7 and also provided in Appendix-I.

5.6.1 User Details

The ten (10) end-users who conducted the SENTINEL trials and fulfilled the online questionnaire (respondents) were representatives of ten (10) external SMEs/MEs headquartered either in Portugal or Greece, reside in Research and Technological Development, IT, Engineering-Energy, Cybersecurity, Food Industry, Wood Product Manufacturing, Indoor Air Quality sectors. The 10 enterprises represent different company types and sizes extending from micro-sized enterprises (MEs) and startups to small and medium enterprises.

In the User Details section, the ten respondents were requested to provide information concerning their position in the organization, their expertise, their cybersecurity and privacy background. The respondents appertain to different organization departments, i.e., R&D, Management, Human Resources, Quality, Cybersecurity and IT and hold either managerial positions (i.e., Co-Founder, Director, Executive coordinator, Administrative, Project Manager) or research-related or technical development-related positions. Their primary area of expertise is related to Technology and Engineering at 50%, IT/Information Security at 20%, Personal Data Protection, Sales & Marketing, Accounting and Finance 10% each, as depicted in Figure 11.

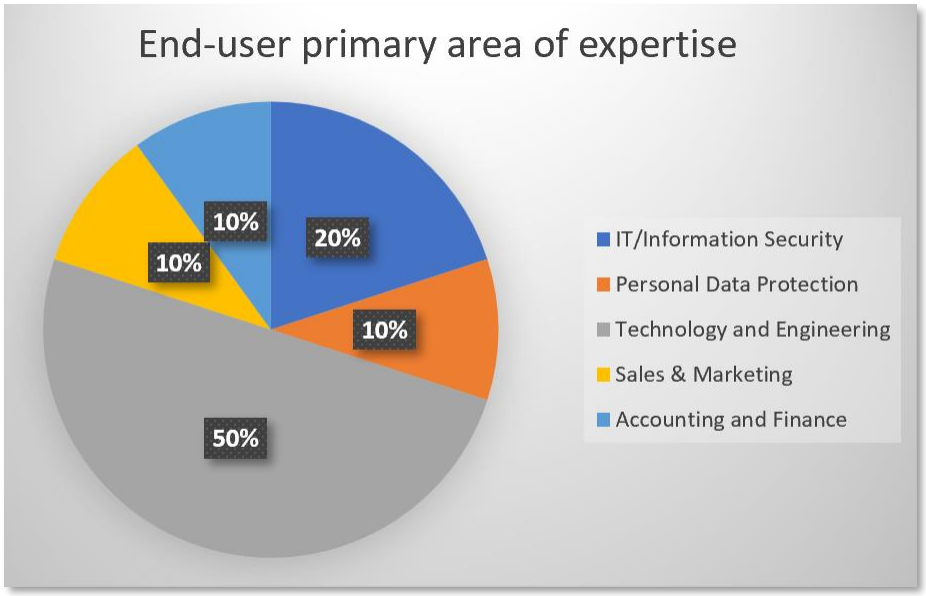


Figure 10. SMEs/MEs end-users' primary area of expertise

Concerning end-users' expertise in cybersecurity, data protection and privacy, 30% of the responses pertain to experts or intermediate level whereas 70% of the responses applied to beginners. This characteristic played a significant role in creating the SENTINEL personas, presented in Section 2.1.

In addition, 2 respondents (20% responses) having either intermediate or expert level in cybersecurity and privacy are currently consulting or executing processes in their organisation related to the implementation of data protection, compliance with GDPR, Access Control, Risk Assessment, implementation of security and privacy control procedures.

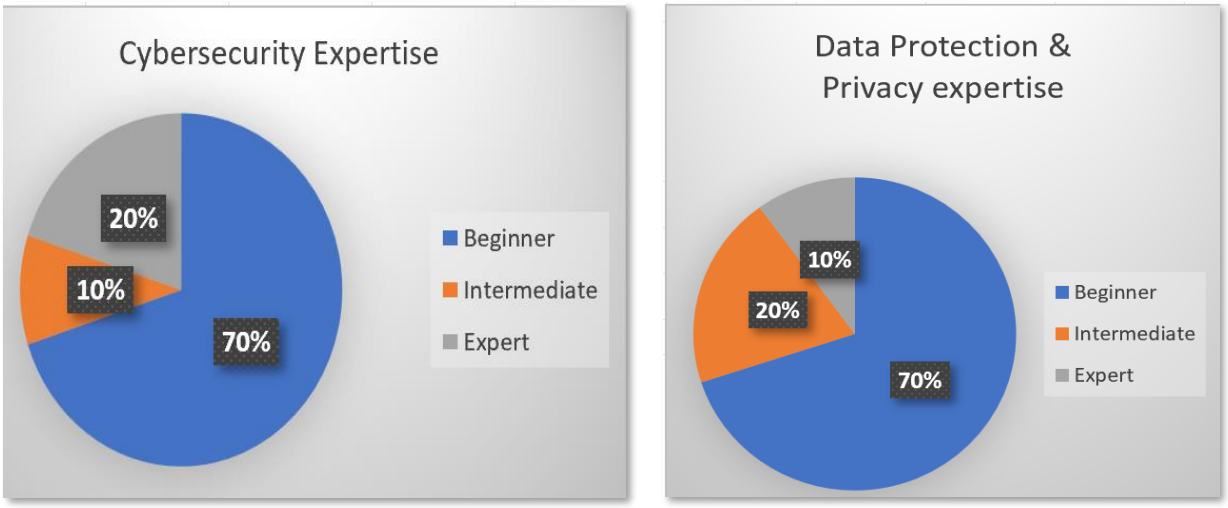


Figure 11. SMEs/MEs end-users' primary area of expertise

According to the questionnaire results, three (3) organisations have annual expenses related to GDPR maintenance of compliance or implementation of OTMs equal to 1-999 € and one (1) organisation equal to 1,000-9,999 €, according to the responses received by the end-users. Moreover, the three (3) respondents answered that their organisations adopt tools/services related to GDPR compliance (either internal software tools or external consulting services) of Annual Licenses type, whereas two (2) organisations undertake annual GDPR compliance audits. The rest of the respondents either answered that they adopt free and open-source tools/services related to GDPR compliance or they didn't provide any relevant information. To this end, an end-user responded that the organisation he/she represents plans to invest in such tools/services in the future.

Furthermore, seven (7) respondents expressed specific concerns regarding cybersecurity and personal data protection in relation to their organization and some answered if they believe that the SENTINEL platform can help to resolve their concerns, as summarized in the following:

- lack of controlling data processing of the numerous projects they perform every day.
- lack of awareness whether the applied controls and established procedures are considered adequate or not for GDPR compliance. The respondent also commented that SENTINEL could help to solve this issue.
- lack of expertise in GDPR domains. The respondent also replied that SENTINEL could help to mitigate this issue.
- not knowing how to maintain security concerning private data after long periods. In addition, the respondent expressed that SENTINEL could help to address this concern.
- privacy and cybersecurity concerns towards specific projects that integrate data from devices to monitoring platforms. The respondent added that the SENTINEL platform can be very useful to encounter this problem.

- lack of knowledge. In addition, the respondent expressed that SENTINEL could raise their cybersecurity and privacy awareness.
- Malware, virus attack, phishing and smishing cyber-attacks concerns. The respondent expressed as well that SENTINEL could help to alleviate such concerns.

Nevertheless, two (2) respondents answered that they don't think their organizations raise any privacy or cybersecurity concern.

5.6.2 User Satisfaction

In this section, the respondents replied to questions related to User Satisfaction quality metric and related sub-metrics, such as *learning/usability capacities* to elicit information considering their level satisfaction after trying the SENTINEL platform.

- Concerning how *easy was to understand and utilise the following main functionalities/services of the SENTINEL platform*:
    - **My Organisation Details**. 5/10 respondents (50%) either strongly agreed or agreed that it was easy to understand and use it, 4/10 respondents (40%) neither agreed nor disagreed and 1/10 respondents (10%) disagreed.
    - **Processing Activity**. 3/10 respondents (30%) either strongly agreed or agreed that it was easy to understand and use it, 5/10 respondents (50%) neither agreed nor disagreed, whereas very few respondents, i.e., 2/10 (20%), strongly disagreed.
    - **Record of Processing Activities (ROPA)**. 3/10 respondents (30%) agreed that it was easy to understand and use it, 4/10 respondents (40%) neither agreed nor disagreed, whereas 1/10 respondents (10%) strongly disagreed and 1/10 respondents (10%) answered “N/A”.
    - **GDPR Compliance Self-Assessment (CSA)**. 4/10 respondents (40%) either strongly agreed or agreed that it was easy to understand and use it, 3/10 respondents (30%) neither agreed nor disagreed, and few respondents, i.e., 3/10 (30%) either disagreed or strongly disagreed with the statement.
    - **Data Protection Impact Assessment (DPIA)**. 5/10 respondents (50%) either strongly agreed or agreed that it was easy to understand and use it, 2/10 respondents (20%) neither agreed nor disagreed, and few respondents, i.e., 3/10 (30%) either disagreed or strongly disagreed with the statement.
    - **Cybersecurity Risk Assessment (CRA)**. 6/10 respondents (60%) agreed that it was easy to understand and use it, 3/10 respondents (30%) neither agreed nor disagreed, and 1/10 respondents (10%) disagreed with the statement.
    - **Acquire policy recommendations**. 5/10 respondents (50%) either strongly agreed or agreed that it was easy to understand and use it, 2/10 respondents (20%) neither agreed nor disagreed, whereas very few respondents, i.e., 2/10 (20%) strongly disagreed and 1/10 respondents (10%) answered “N/A”.

  - **Exploring the Observatory**. 6/10 respondents (60%) either strongly agreed or agreed that it was easy to understand and use it, 3/10 respondents (30%) neither agreed nor disagreed, whereas 1/10 respondents (10%) answered “N/A”.
  - **Reporting Incidents**. 6/10 respondents (60%) either strongly agreed or agreed that it was easy to understand and accomplish in the SENTINEL platform, 2/10 respondents (30%) neither agreed nor disagreed, whereas 1/10 respondents (10%) disagreed and 1/10 respondents (10%) answered “N/A”

- Regarding whether the SENTINEL **experiment workflow** was streamlined and easy to follow, 6/10 respondents (60%) either strongly agreed or agreed, 2/10 respondents (20%) neither agree or disagree, whereas very few respondents, i.e., 2/10 respondents (20%), disagreed or answered “N/A”.
- Concerning whether SENTINEL provides **efficient guidance and help menu** to allow the user to conduct privacy assessments, 4/10 respondents (40%) either strongly agreed or agreed, 4/10 respondents (40%) neither agreed nor disagreed, and very few respondents, i.e., 2/10 (20%) answered “N/A”.
- 6/10 respondents (60%) either strongly agreed or agreed that “SENTINEL **Recommendations** to SMEs/MEs for undertaking OTMs (Policy Draft) to increase their level of security and GDPR compliance are described accurately and clearly, whereas very few respondents, i.e., 2/10 respondents (20%), neither agreed nor disagreed, and very few respondents, i.e., 2/10 respondents (20%), disagreed or strongly disagreed.
- Regarding the **Dashboard Menu**, 6/10 respondents (60%) either strongly agreed or agreed that it was easy to understand and use it, 3/10 respondents (30%) neither agreed nor disagreed, and 1/10 respondents (10%) strongly disagreed.
- With respect to the SENTINEL platform **visualization capabilities**, 4/10 respondents (40%) either strongly agreed or agreed that are *helpful and sufficient* and that the SENTINEL platform provides interactive control of the working process, reports, dashboard help menu and tooltips, whereas 5/10 respondents neither agreed nor disagreed, and 1/10 respondents (10%) disagreed.

Pertaining to the SENTINEL platform *performance efficiency in terms of speed*:

- 5/10 respondents (50%) either strongly agreed or agreed that are satisfied when filling **My Organisation Details**, whereas 4/10 respondents (40%) neither agree or disagree, and 1/10 respondents (10%) replied as N/A.
- 5/10 respondents (50%) either strongly agreed or agreed that are satisfied when creating a **PA**, 4/10 respondents (40%) neither agree or disagree, whereas 1/10 respondents (10%) strongly disagreed and 1/10 respondents (10%) answered “N/A”.
- 4/10 respondents (40%) agreed that are satisfied when using the **ROPA**, 5/10 respondents (50%) neither agreed nor disagreed, and 1/10 respondents (10%) answered “N/A”.

- 4/10 respondents (40%) agreed that are satisfied when executing the **GDPR CSA**, 5/10 respondents (50%) neither agreed nor disagreed, and 1/10 respondents (10%) answered "N/A".
- 4/10 respondents (40%) agreed that are satisfied when executing the **DPIA**, 3/10 respondents (30%) neither agreed nor disagreed, very few, i.e., 2/10 (20%), disagreed and 1/10 respondents (10%) answered "N/A".
- 6/10 respondents (60%) agreed that are satisfied when executing the **CSRA**, 3/10 respondents (30%) neither agree or disagree, and 1/10 respondents (10%) answered "N/A".
- 4/10 respondents (40%) agreed that are satisfied when **acquiring policy recommendations**, 4/10 respondents (40%) neither agreed nor disagreed, whereas 1/10 respondents (10%) disagreed, and 1/10 respondents (10%) answered "N/A".
- 6/10 respondents (60%) agreed that are satisfied when **exploring the Observatory**, 3/10 respondents (30%) neither agreed nor disagreed, and 1/10 respondents (10%) answered "N/A".
- 6/10 respondents (60%) either agreed that are satisfied when **reporting incidents**, 3/10 respondents (30%) neither agreed nor disagreed, and 1/10 respondents (10%) answered "N/A".
- Concerning the approximate time required to complete the experiment's workflow, 4/10 respondents (40%) spent ≤ 30 min. to undertake the SENTINEL experiment, whereas 1/10 respondents (10%) spent ≤ 60 min., 1/10 respondents (10%) spent < 60 min. and 4/10 respondents (40%) replied as N/A (cf. Figure 12).

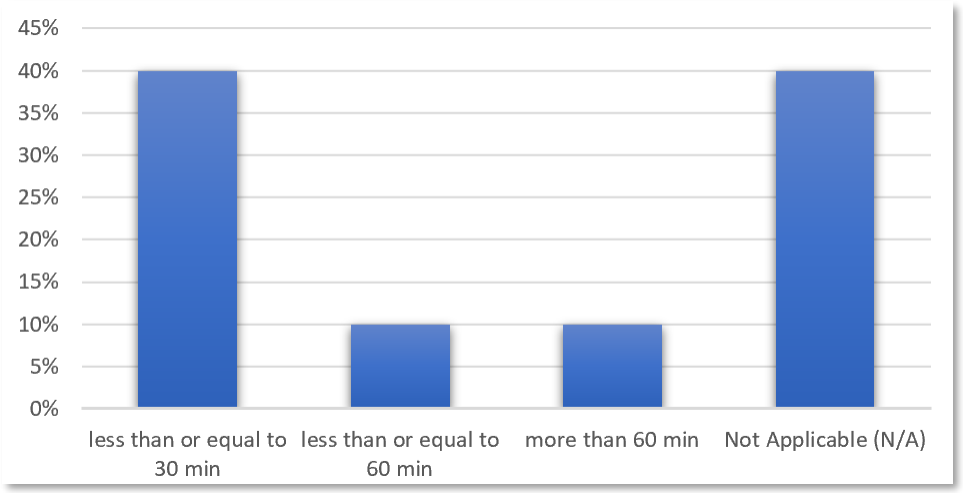


Figure 12. Approximate time end-users needed to fulfil the SENTINEL experiment

- Regarding whether the "*SENTINEL platform gave error messages that clearly told the end-user how to fix problems*", 2/10 respondents (20%) agreed with the statement, 3/10

respondents (30%) neither agreed nor disagreed, 3/10 respondents (30%) and 2/10 respondents (20%) replied as N/A

In addition, three (3) respondents provided suggestions for improving the SENTINEL platform's functionalities:

- The design and look are clean, clear, and simple. Nonetheless, the dashboard is too crowded and it could be customized in order to deal with the several existing functionalities.
- There should be indications of the elements that are missing and must be fulfilled to complete an analysis.
- "The vocabulary used is domain-specific, hard to understand for a basic user.

5.6.3 User Interface/User Experience (UI/UX)

In the current section the respondents answered questions related to the UI/UX of the SENTINEL platform. The feedback received by the end-users is presented in the following.

- 9/10 respondents (90%) either strongly agreed or agreed that the characters on the screens are easy to read and 1/10 respondents (10%) answered “N/A”.
- 8/10 respondents (80%) either strongly agreed or agreed that the language used in SENTINEL is comprehensive, whereas very few respondents, i.e., 2/10 (20%), disagreed with the statement.
- 6/10 respondents (60%) either strongly agreed or agreed that the information (i.e. on-screen messages, and other documentation and tooltips) provided with the dashboard is accurate and clear. However, 3/10 respondents (30%) neither agreed nor disagreed and 1/10 respondents (10%) disagreed with the statement.
- 7/10 respondents (70%) either strongly agreed or agreed that “the organization of information on the SENTINEL screens is clear and user-friendly”. Very few respondents, i.e., 2/10 (20%), neither agreed nor disagreed and 1/10 respondents (10%) disagreed with the statement.
- 6/10 respondents (60%) either strongly agreed or agreed that “SENTINEL has clearly marked way-finding buttons” and 4/10 respondents (40%) neither agreed nor disagreed with the statement.
- 6/10 respondents (60%) either strongly agreed or agreed that “the use of terms throughout SENTINEL is consistent”, whereas 4/10 respondents (40%) neither agreed nor disagreed with the statement.
- 5/10 respondents (50%) either strongly agreed or agreed that “the position of messages on the screens is proper”, whereas 4/10 respondents (40%) neither agreed nor disagreed and 1/10 respondents (10%) disagreed with the statement.

- 8/10 respondents (80%) either strongly agreed or agreed that “the different screens of SENTINEL are cohesive in look-and-feel” and very few respondents, i.e., 2/10 (20%), neither agreed nor disagreed with the statement.
- 7/10 respondents (70%) either strongly agreed or agreed that “the interface of SENTINEL is pleasant”, nevertheless, very few respondents, i.e., 2/10 (20%), neither agreed nor disagreed and 1/10 respondents (10%) strongly disagreed with the statement.
- 4/10 respondents (40%) either strongly agreed or agreed that “the SENTINEL templates helped them to identify and record their organisation's Processing Activities”, whereas 5/10 respondents (50%) neither agreed nor disagreed and 1/10 respondents (10%) disagreed with the statement.
- 5/10 respondents (50%) either strongly agreed or agreed that “SENTINEL overall provides all the functions and capabilities they expect to have for assessing privacy of their organisation's Processing Activities” whereas 5/10 respondents (50%) neither agreed nor disagreed with the statement.

Furthermore, a respondent commented that in some cases, manually scroll up is needed to the top to see the progress/error messages.

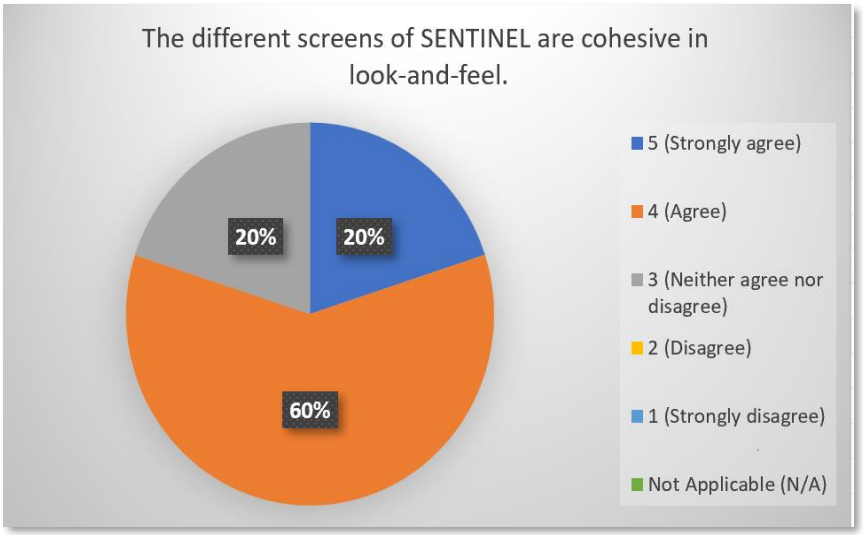


Figure 13. End-user responses for SENTINEL screens I

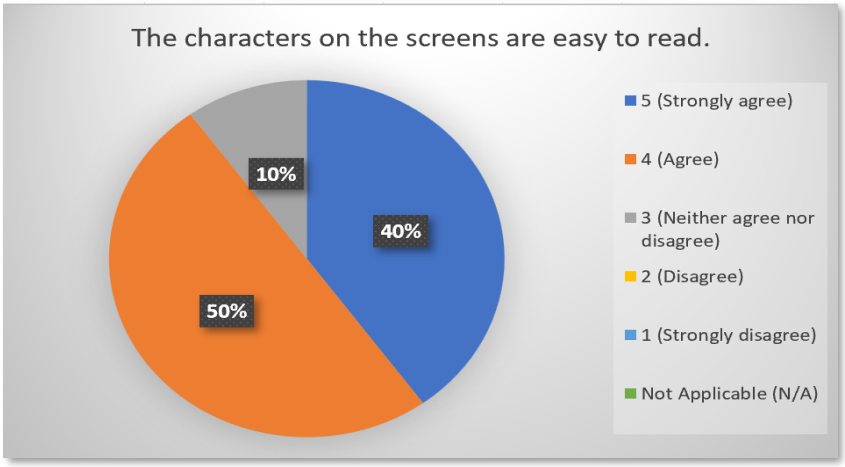


Figure 14. End-user responses for SENTINEL screens II

5.6.4 CyberRange Gaming

This section captures questionnaire's responses concerning the CyberRange Gaming environment of SENTINEL.

- 5/10 respondents (50%) either strongly agreed or agreed that it was easy to understand and test the CyberRange Gaming, whereas 1/10 respondents (10%) neither agreed nor disagreed, 1/10 respondents (10%) disagreed with the statement. The rest of the respondents replied as N/A.
- 3/10 respondents (30%) either strongly agreed or agreed that the CyberRange Gaming has helped them to explore different types of threats and attacks related to data storage and accessibility. Nevertheless, very few respondents, i.e., 2/10 (20%), neither agreed nor disagreed and 1/10 respondents (10%) disagreed with the statement. The rest of the respondents replied as N/A.
- 3/10 respondents (30%) either strongly agreed or agreed that the CyberRange Gaming has helped them to acquire good practices to better protect their data, whereas very few respondents, i.e., 2/10 (20%), neither agreed nor disagreed, 1/10 respondents (10%) disagreed with the statement and the rest of the respondents replied as N/A.
- 4/10 respondents (40%) agreed that the CyberRange Gaming has helped them to detect, analyse and better understand vulnerabilities on ICT assets, 1/10 respondents (10%) neither agreed nor disagreed, 1/10 respondents (10%) disagreed and 4/10 respondents (40%) answered "N/A".

Moreover, two (2) respondents provided textual feedback from their CyberRange Gaming experience suggesting areas of improvement:

- A respondent commented that the adoption of CyberRange Gaming is a "good idea". Nevertheless, some challenges are difficult to activate. In addition, he/she replied that there is too much information/text and graphics which could be simplified and that the access to the actual practices and instructions could be more clearly accessible to be

aligned with the overall clean feel that the SENTINEL platform provides. To this end, he/she mentioned to alter the sound capacity.

- Another respondent indicated that English language should be supported.

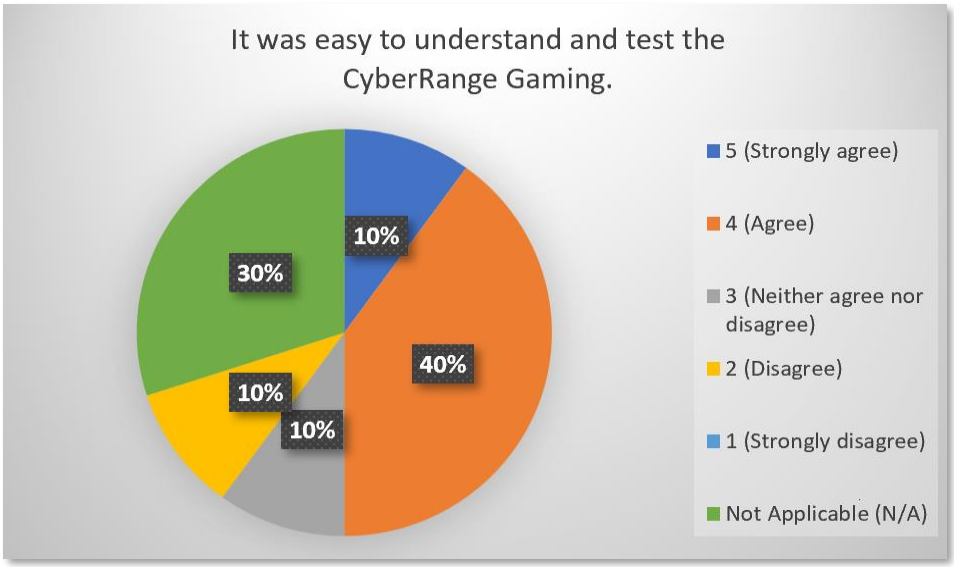


Figure 15. End-user responses for understanding and testing the CyberRange Gaming

5.6.5 Security and Results Quality, Personal Data Protection and Compliance

In this section, the respondents answered questions related to security and quality of results, personal data protection and compliance. The feedback gathered is provided below.

- Concerning *SENTINEL OTMs/ recommendations*:
    - 4/10 respondents (40%) either strongly agreed or agreed that the SENTINEL measures/recommendations increase GDPR compliance of the experiment's Processing Activity in an efficient manner, whereas 3/10 respondents (30%) neither agreed nor disagreed and the rest of the respondents replied as N/A
    - 5/10 respondents (50%) either strongly agreed or agreed that “the SENTINEL measures/recommendations can assure privacy of related data”. However, 4/10 respondents (40%) neither agreed nor disagreed with the statement and 1/10 respondents (10%) answered “N/A”.
    - 7/10 respondents (70%) either strongly agreed or agreed that privacy incidents can be prevented by implementing SENTINEL recommendations, whereas 1/10 respondents (10%) neither agreed nor disagreed and 2/10 respondents (10%) as well answered “N/A”.
    - Three (3) respondents commented favorably that SENTINEL measures/ recommendations/suggested tools/techniques can be utilised to increase the security and privacy of their Processing Activities. Specifically, an end-user remarked that he/she received notification of missing procedures and controls, and

recommendation for opensource tools and training material for further reading and understanding.

- Seven (7) respondents commented encouragingly that the SENTINEL measures/recommendations received, could mitigate the risks/threats identified within their experiment.

- With respect to the SENTINEL Cybersecurity simulation environment:
  - Seven (7) respondents replied positively that it helped them to identify risks/threats to the registered assets. One of those respondents added that he/she delivered "a vulnerability list depending on the device in place".
  - Six (6) respondents commented that it helped them to identify possible attack scenarios.

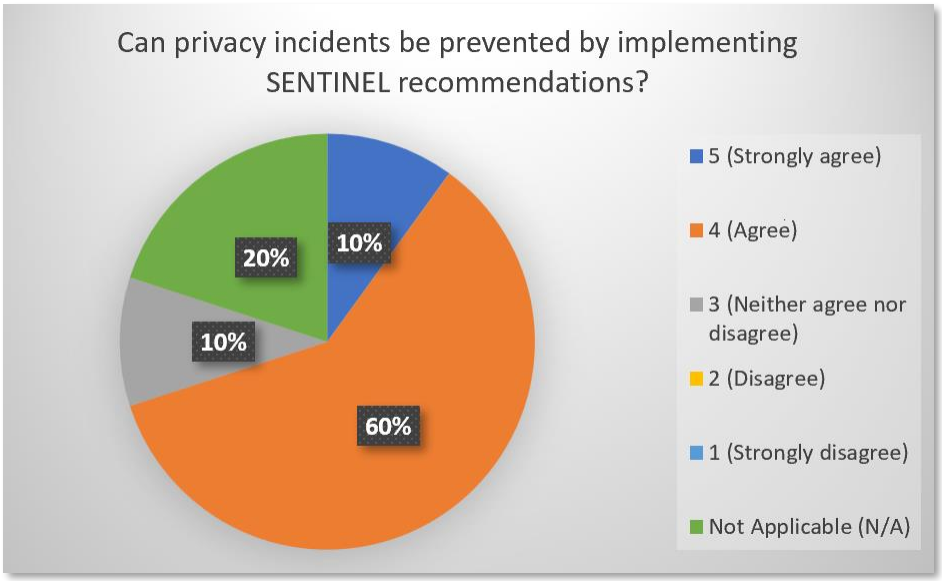


Figure 16. End-user responses whether privacy incidents can be prevented via implementing SENTINEL recommendations

5.6.6 Business Performance

The current section contains respondents feedback gained after answering questions pertaining to business performance.

- 6/10 respondents (60%) either strongly agreed or agreed that the SENTINEL services can help address challenges they face in their organisation with respect to privacy and cybersecurity, whereas 2/10 respondents (20%) neither agreed nor disagreed and 2/10 respondents (20%) as well replied as N/A

- 4/10 respondents (40%) either strongly agreed or agreed that they did not face any interruptions while using the SENTINEL platform. Though, whereas 3/10 respondents (30%) neither agreed nor disagreed, very few respondents, i.e., 2/10 (20%), disagreed and 1/10 respondents (10%) answered "N/A".

- 5/10 respondents (50%) either strongly agreed or agreed that SENTINEL can be utilised for all processing activities and assets used for data storage and accessibility in their organisation. Moreover, 4/10 respondents (40%) neither agreed nor disagreed with the statement and 1/10 respondents (10%) answered “N/A”.
- Concerning the measures recommended by SENTINEL:
    - 6/10 respondents (60%) either strongly agreed or agreed that they can improve the cybersecurity of all stored data, whereas 2/10 respondents (20%) neither agreed nor disagreed with the statement and 2/10 respondents (20%) answered “N/A”.
    - 5/10 respondents (50%) either strongly agreed or agreed that they can improve implementation of controls that limit any type of unauthorized access to the data. Furthermore, 3/10 respondents (30%) neither agreed nor disagreed with the statement and 2/10 respondents (20%) answered “N/A”.
    - 7/10 respondents (70%) either strongly agreed or agreed that they can improve the security of information/data exchange, whereas very few respondents, i.e., 2/10 (20%), neither agreed nor disagreed with the statement and 1/10 respondents (10%) replied as “N/A”.
    - 8/10 respondents (80%) either strongly agreed or agreed that SENTINEL measures/recommendations can improve the maintenance and retention of data. Furthermore, 1/10 respondents (10%) neither agreed nor disagreed with the statement and 1/10 respondents (10%) answered “N/A”.
- 5/10 respondents (50%) either strongly agreed or agreed that the “SENTINEL platform is easy to learn”. Nevertheless, 2/10 respondents (20%) neither agreed nor disagreed and the rest either disagreed or strongly disagreed.
- 4/10 respondents (40%) are satisfied with the time needed to complete the privacy assessment (GDPR CSA and DPIA) and receive recommendations, whereas 2/10 respondents (20%) neither agreed nor disagreed, 3/10 respondents (30%) either disagreed or strongly disagreed with the statement and 1/10 respondents (10%) replied as “N/A”.
- 5/10 respondents (50%) either strongly agreed or agreed that “SENTINEL simplifies privacy assessment compared to the tools/services they are currently using”. Nonetheless, 3/10 respondents (30%) either disagreed or strongly disagreed, 1/10 respondents (10%) strongly disagreed with the statement and 1/10 respondents (10%) answered “N/A”.
- 4/10 respondents (40%) agreed that “SENTINEL simplifies cybersecurity risk analysis compared to the tools/services they are currently using”. However, 3/10 respondents (30%) either disagreed or strongly disagreed and the rest replied as “N/A”.
- 4/10 respondents (40%) either strongly agreed or agreed that “the measures recommended by SENTINEL will improve the effectiveness of their organisation regarding

cybersecurity and personal data protection processes completion". Nevertheless, 4/10 respondents (40%) either disagreed or strongly disagreed and the rest replied as "N/A".

- 4/10 respondents (40%) agreed that "using SENTINEL will not necessitate additional human and/or financial resources (e.g. hiring external cybersecurity analysts and privacy experts) from their organisation". Moreover, 2/10 respondents (20%) neither agreed nor disagreed, 2/10 respondents (20%) either disagreed or strongly disagreed and the rest answered "N/A".
- 5/10 respondents (50%) either strongly agreed or agreed that "*using SENTINEL has helped them understand their organisations' GDPR compliance requirements*". However, 3/10 respondents (30%) neither agreed nor disagreed and the rest respondents answered "N/A".
- 6/10 respondents (60%) either strongly agreed or agreed that "SENTINEL can help them form their organisations' cybersecurity and personal data protection strategy, whereas 2/10 respondents (20%) neither agreed nor disagreed, 1/10 respondents (10%) disagreed with the statement and 1/10 respondents (10%) replied as "N/A".

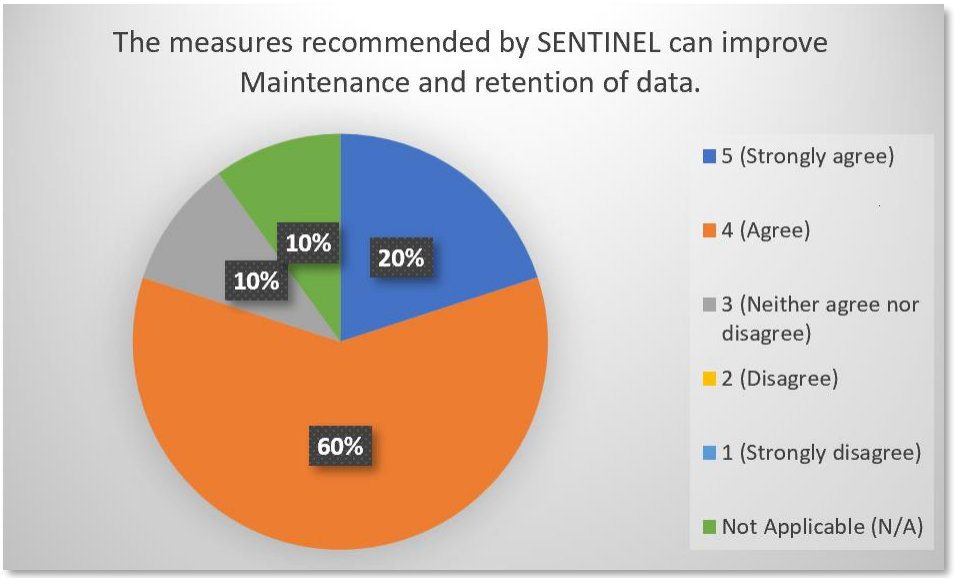


Figure 17. End-user responses regarding SENTINEL recommended measures.

5.6.7 Express end-user opinion and additional comments

This last section of the User Evaluation Questionnaire aims to allow end-users to express their opinion after trying SENTINEL and provide further textual feedback with suggestions for future improvements. To this objective, all information collected from the DIH pilot end-users is presented in the following.

- Concerning the question to describe on *the quality of SENTINEL privacy assessments (GDPR CSA and DPIA) results in general:*

- Four (4) end-users responded positively and endorsed the SENTINEL platform with comments, such as "*the results look very promising*", "*It is a good tool to protect the organisation requirements*" and characterised SENTINEL "*Very good*", "*Appealing".*
- An end-user commented that he/she couldn't' provide a full assessment during the trials and thus could not utilise their relevant capabilities.
- Another end-user characterised the SENTINEL platform is complex. And hinders measure the quality of the results.

- With reference to the question of describing *the quality of SENTINEL cybersecurity risk analysis*:
  - Five (5) end-users replied positively using characterisations, such as "*Very good"*, "*a good platform to evaluate access, changes, or destroyed sensitive information*".
  - One (1) end-user pointed out that CRA are focused on CVE cybersecurity vulnerabilities characteristics [9] and specific pre-defined list of devices. The end-user proposed to enhance this information with additional open sources to cover sector-specific security requirements, such as of a healthcare institution.

- Regarding the question to *specify any issues (e.g., bugs, content, layout, design, errors, etc.) the end-users faced while utilising the SENTINEL functionalities and testing the platform*:
  - Four (4) end-users did not find any issues to specify.
  - An end-user described that he/she could not add an asset because it was not possible to insert the name of the responsible person in the form which hindered the process of receiving recommendations and continuing with the use of additional features.
  - An end-user commented that he/she could not add new assets.
  - An end-user annotated that devoted too much time loading some combo-box, page freezes.

- Regarding the description of the most positive aspects of the SENTINEL platform considering its functionalities:
  - Three (3) end-users found most useful the policy recommendations functionalities of the SENTINEL platform. One of them continued expressing that Policy Recommendations could be enhanced with further details on "*the measures required, backed up with cybersecurity, privacy and related policy & compliance monitoring*" and to allow the users gain an overall understanding.
  - An end-user found most positive the raise of awareness on their organisation's cybersecurity and risks the SENTINEL functionalities provided.
  - Another end-user commented that the SENTINEL platform is "useful in terms of learning and testing knowledge" and he/she acknowledged the idea behind that

recommendations and GDPR compliance tool analysis are a must to any organisation

- An additional end-user characterised "*accessibility*" as the most positive aspect of SENTINEL.

- The end-users were kindly requested to describe additional services/capabilities that they would like to see in the SENTINEL platform, according to their specific requirements:
  - An end-user described the need to *"adapt to various types of processes and research studies in healthcare. Medical devices, such as sensors or Internet of Medical Things (IoMT), can have many unknown security problems or difficult to solve*".
  - Another end-user suggested to focus on "*Industrial Internet of Things (IIot) security and cloud security*".
  - An end-user indicated to target on more focused recommendations.
  - Nevertheless, three (3) end-users replied that they *did not notice any need besides what SENTINEL already offers.*

- At last, the end-users were asked to provide further comments/suggestions for improvements after your experience with SENTINEL.
  - An end-user encouraged for UI/UX improvements in terms of becoming more user-friendly.
  - Another end-user proposed to "*confirm needs and preferences with end-users and if possible, co-design the solution with them*".
  - An end-user highlighted the need of *enhancing the SENTINEL platform with explanatory hints* for *privacy/security related terms* to facilitate the comprehension of GDPR and cybersecurity terminology utilised, in case SENTINEL is used by SMEs/MEs employees that may *lack privacy and cybersecurity expertise* (SENTINEL may not address only Data Protection Officers (DPOs) and privacy/cybersecurity experts)
  - Another end-user stated that it could be very useful and applicable to several industry domains, in case of *integrating IIoT security*.

6. SENTINEL pilot evaluation outcomes, KRs/KPIs progress and monitoring

One of the main activities of task T6.2 was to execute the user-centric evaluation methodology that drives the entire evaluation process of SENTINEL. This section provides an overview of the ongoing evaluation advancements and monitoring within SENTINEL. In particular, it describes the SENTINEL pilot overall results and the evaluation KRs/KPIs progress.

6.1 SENTINEL pilot overall results

The table below provides a synopsis of the favourable feedback from the pilot results and areas for improvement. A positive response is defined as a situation where the percentage of "Agree" or "Strongly agree" responses surpasses the percentage of “Neither Agree nor Disagree”, "Disagree" or "Strongly disagree" responses (N/A answers not counted).

Part A - User Satisfaction		
Category Name	**Positive Feedback**	**Suggestions/ Room for improvements**

Usability, Time Efficiency, Functional Suitability and System Performance	• Easy to understand and accomplish:
	  ○ My Organisation Details
	  ○ CSRA
	  ○ Policy Recommendations
	  ○ Observatory
	  ○ Reporting Incidents
	• The experiment workflow was streamlined and easy to follow.
	• SENTINEL Recommendations to SMEs/MEs for undertaking technical and organisational measures (Policy Draft) to increase their level of security and GDPR compliance are described accurately and clearly.
	• It was easy to understand the structure and logic of the SENTINEL Dashboard Menu and easy to use.
	• Satisfactory performance of the SENTINEL platform.
		• Use of the ROPA
		• How to acquire policy recommendations
		• Content and terminology.
		• Dashboard is too crowded. A customisable dashboard would be desirable.
		• Elements that are missing and must be fulfilled in order to complete an analysis are not always clearly indicated.
		• Too much domain specific vocabulary used, which is hard for a basic user to understand.
		• Recommendations are not readily accessible. Multiple drop-down menus required.
		• OTM's do not appear to be specific.
		• Observatory looks aimed at IT professionals rather than beginner or intermediate.

User Interface/User Experience (UI/UX)	• The characters on the screens are easy to read. • The language used in SENTINEL is comprehensive. • The information (i.e. on-screen messages, and other documentation and tooltips) provided with the dashboard is accurate and clear. • The organization of information on the SENTINEL screens is clear and user-friendly.	• Manual scroll up to the top required to see the progress/error messages in some cases. • Can be a bit overwhelming for someone who reviews these things annually.

	• SENTINEL has clearly marked way-finding buttons (exit, back, next page, etc.) • The use of terms throughout SENTINEL is consistent. • The position of messages on the screens is proper. • The different screens of SENTINEL are cohesive in look-and-feel. • The interface of SENTINEL is pleasant.	
CyberRange Gaming	• It was easy to understand and test the CyberRange Gaming. • The CyberRange Gaming has helped me to detect, analyse and better understand vulnerabilities on ICT assets.	• Does not work well in all browsers. • Often freezes. • Too much information/text and graphics and the access to real practices and instructions is not clear. • It does not agree with the clean feel of the sentinel platform. • The sound can be annoying for some. • Cyber Range Gaming is in mixed languages - not English as expected.
Results, Security, Quality, Personal Data Protection and Compliance	• SENTINEL measures/recommendations can increase GDPR compliance of Processing Activities in an efficient manner. • SENTINEL measures/recommendations can assure privacy of related data. • SENTINEL Cybersecurity simulation environment has helped to identify risks/threats to registered assets. • SENTINEL measures/ recommendations can mitigate risks/threats identified. • SENTINEL Cybersecurity simulation environment has helped to identify possible attack scenarios. • Privacy incidents can be prevented by implementing SENTINEL recommendations.	• No recommendations/ suggested tools/ techniques that can be utilised to increase the security and privacy of your Processing Activities were found. • SENTINEL platform is not easy to learn. • Time needed to complete the privacy assessment (A GDPR Compliance Self-Assessment and Data Protection Impact Assessment) and receive recommendations. • Using SENTINEL will necessitate additional human and/or financial resources (e.g. hiring external cybersecurity analysts and privacy experts).

Business Performance	• The SENTINEL services can help address challenges in an organisation with respect to privacy and cybersecurity.
	• The measures recommended by SENTINEL can improve:
	  ○ Cybersecurity of all stored data
	  ○ Implementation of controls that limit any type of unauthorized access to the data
	  ○ Security of information/data exchange
	  ○ Maintenance and retention of data	

	• SENTINEL can be used for all processing activities and assets used for data storage and accessibility in my organisation. • SENTINEL simplifies privacy assessment (GDPR Compliance Self-Assessment and Data Protection Impact Assessment) compared to tools/services currently used. • SENTINEL simplifies cybersecurity risk analysis compared to tools/services currently used. • The measures recommended by SENTINEL will improve the effectiveness of an organisation regarding cybersecurity and personal data protection processes completion. • SENTINEL helps understand an organisations' GDPR compliance requirements. • SENTINEL helps to form an organisations' cybersecurity and personal data protection strategy.	
Part B – User opinions		
Category Name	**Positive Feedback**	**Suggestions/ Room for improvements**

Express end-users opinion and additional comments	• The quality of SENTINEL privacy assessments (GDPR Compliance Self-Assessment and Data Protection Impact Assessment) results in general can be described in general:
	  ○ Helpful, very promising, appealing.
	  ○ A good tool to protect the organisation requirements.
	• Insight into GDPR and its necessity.
	• Useful in terms of learning and testing knowledge.
	• Recommendations found most positive functionality.
	• Awareness of cybersecurity and risks.
		• The quality of SENTINEL cybersecurity risk analysis is very focused on CVEs and specific pre-defined list of devices.
		• Useful tool, but mainly for IT professionals.
		• Errors and freezing whilst using platform.
		• Assets cannot be added easily in some occasions (e.g. it was not possible to insert a name for the responsible person in the form).
		• Clearer terminology and working game.
		• More focused recommendations.
		• Industrial Internet of things (IIot) security and cloud security coverage.
		• More user friendly.
		• Explanatory hints could be used the privacy- and security-related terms.

		• Trying to do too many things. Maybe separate modules for security and GDPR.

6.2 Evaluation KRs/KPIs progress

The current status of the SENTINEL KRs/KPIs associated with the SENTINEL user-centric evaluation is presented in the table below. It should be mentioned that the final KRs/KPIs assessment for each demonstrator both in operational (cost, service levels, etc.) and technical terms (performance of solution) is going to be documented in deliverable "D6.3 - Assessment report and impact analysis" (M36).

KR-1.1: Successful integration and orchestration of SENTINEL technology offerings. Owner: **INTRA**
The refined architecture, as presented in D1.2, was designed to accommodate all SENTINEL offerings as well as providing the means for incorporating external ones in the form of plugins. Due to an integration-first approach that has been followed throughout the project development, interfaces and messaging formats as well as sequence diagrams have been defined and documented. As a result, we are confident that all project technologies have been fully and successfully integrated on time. This was reflected on the MVP, presented in D5.4, as well as the Full-Featured Version (FFV), described in D5.5 and finalised in D5.6 delivered in M30. This KR is considered ~100% achieved.
KR-1.2: 40% improved compliance efficiency for SMEs/MEs. Owner: **LIST**
Efficiency indicates how consistently things are done right. Applied to SENTINEL, measuring efficiency requires calculating the rate at which an SME can complete the assessment of all their personal data processing activities (PAs), which, in turn requires comparing the number of PAs for which compliance with GDPR has been established/assessed to the total of PAs the company is accountable for. This is calculated as follows: $Compliance\ efficiency$ = $(PAs\ assessed/\ Total\ PAs) * 100$ By providing innovative and user-centric data protection services such as the ROPA, GDPR CSA and DPIA, SENTINEL is expected to boost compliance efficiency by at least 40 percentage points. To establish this KR, it is first necessary to compare for each user of SENTINEL evolution of their compliance efficiency rate. To do so, compliance efficiency will be measured twice: before using SENTINEL (t0), and after a period of use (t1). KR-1.2 will result in the average of the variation of compliance efficiency rate of SENTINEL users (n). KR1.2 = $\sum Compliance\ efficiency\ (t1) - Compliance\ efficiency\ (t0)$ So far, the work conducted in WP6 indicate that around 18 end-users have already tested the ROPA, GDPRCSA and DPIA services of the platform upon specific pilot experiments of at least 6 different PAs utilised in the company's normal operations. The compliance efficiency that SENTINEL can provide to SMEs/MEs is going be assessed in the M30-M36 period as the SENTINEL compliance services are planned to be demonstrated and tested by a set of additional trials organised for additional external SME end-users engaged in the scope of the final SME-centric workshop envisioned for M33 (February 2024). This approach will allow the consortium to measure the compliance efficiency that SENTINEL can provide to the engaged SMEs after distinct periods of use and make comparisons with the efficiency rate the SMEs had obtained before using SENTINEL by utilising the compliance efficiency indicators presented above. KR is considered ~70% achieved.
KR-1.3: Reduction of compliance – related costs by at least 40%- against benchmarks defined by stakeholders and EU (International) initiatives. Owner: **STS**
This KR is closely associated with KR-1.2. It is crucial to establish the average cost of compliance for SMEs before its implementation. A forthcoming survey, with a specific focus on cost-related data during a planned workshop alongside the 7th plenary meeting, combined with literature data acquired in the project's initial year, will facilitate the identification of average GDPR compliance costs for SMEs. This

data will establish a baseline for comparison against the SENTINEL offerings. Additionally, during a workshop among SENTINEL partners, with the support of the Horizon Results Booster Service 2, a baseline for the pricing of the SENTINEL platform can be determined, allowing for a direct comparison with compliance-related costs. The complete achievement of this KR is expected in the final months of RP2. Currently, this KR is considered approximately 50% achieved.

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

Regarding KR-1.4, SENTINEL has organized four (4) SME-centric workshops (September 2021, May 2022, October 2022 and September 2023), with the objective of raising awareness in SMEs/MEs all over the EU about GDPR compliance and PDP. Within this context, the SENTINEL offerings have been identified at an early stage of the project, so as to start motivating attendees and grasping their attention towards the project's tools and compliance services. Based on the established list of offerings, the SENTINEL consortium has prepared a questionnaire to record user acceptance of SENTINEL offerings which will serve as a baseline.
During the 3rd workshop where the SENTINEL MVP demonstration took place 29% of participants accepted that SENTINEL can be a potential solution to be implemented in their companies, 42% have answered that they could consider investing in tools/services similar to SENTINEL within the next 2 years, while 54% choose that the "Automated GDPR compliance, recommendation and real-time monitoring" are the most useful services among the SENTINEL tools to be used in their own business. During the 4th workshop where the SENTINEL FFV demonstration took place, with 24 invited SMEs, we repeated the questionnaire with improvements regarding the context and 20% of participants accepted that SENTINEL can be a potential solution to be implemented in their companies, 35% have answered that they could consider investing in tools/services similar to SENTINEL within the next 2 years, while 55% choose that the "A toolkit for evidence-based GDPR compliance" is the most useful services among the SENTINEL tools to be used in their own business. Nevertheless, we plan to organise one final SME-centric workshop and try to invite both new attendees as well as already engaged participants to measure this KR. So far, we achieved 40% completion of this specific KR.

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

With the CyberRange Gaming interface the end-users have interact with a simulated SME environment and learn how to protect personal and sensitive data. They see a phishing attack that can lead to Identity theft, malware installation, financial fraud, credential harvesting and data breaches. They also see the risk of not protected their files that can lead to unauthorized access with legal, reputational or commercial consequences. They learn the consequence of social media exposure with social engineering attack that can lead to several cyber risk like data breaches, identity theft, phishing attacks and cyberbullying. They also learn the importance of password policy, with a real example of a Local File Inclusion attack.

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

Starting from the MVP phase, the SENTINEL Recommendation Engine (RE) was implemented following a rule-based approach to provide a set of recommendations depending on cases of profile and risk level outputs. It leverages a pre-specified rule base to map Organisational and Technical Measures (OTMs) that correspond to a given risk assessment level with a list of plugins, trainings and other optional capabilities. At the FFV phase, SENTINEL RE was further extended with over 50 open-source tools and around 120 courses to increase flexibility and accuracy of recommendations. Additionally, asset ownership and locality were introduced in the calculations making the RE more accurate and realistic. This KR is considered ~100% achieved.

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

The KR-2.3 is linked to WP2 and 4, and more specifically deliverables D2.1 and D4.1 due M12 and D2.2, D2.3, D4.2 and D4.3 due in M18 and M30 respectively. A lot of progress has been made already regarding this KR as part of MVP and FFV versions of the GDPR CSA and DPIA self-assessment tools

respectively were designed and implemented. Both tools are designed, implemented and fully integrated into the SENTINEL platform via APIs and can be executed for one processing activity at a time, providing a score that will be visible to the user via MySentinel UI. Both frameworks were tested in real-world settings during the workshops organised under WP6. A conformity assessment of the GDPR CSA Assessment Model has been performed with CARPA's data protection requirements, while in parallel assessments of the GDPR CSA Method, Framework and Model have been performed with ISO/IEC 33002, ISO/IEC 33003 and ISO/IEC 33002 respectively. This KR is considered ~100% achieved

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

The SENTINEL IdMS provides authentication, authorization and Single Sign-On capabilities to SENTINEL end users, based on an open-source solution (Keycloak), towards adopting the MyData model, whose core idea is that data owner should have an easy way to see where personal data goes, specify who can use it, and alter these decisions over time. It is offered as-a-service, where SMEs can use it to verify, and manage attributes and entitlements that are necessary for the creation and maintenance of digital identities for all users accessing third party applications EU-wide. This includes functionalities and flows like user registration, account recovery, profile management, credentials management, and consent management. In terms of record keeping, SENTINEL offers the capability of storing versatile organisation-wide information, as well as storage of activities that involve processing personal data. Furthermore, it offers the capability of keeping a formal, immutable and auditable Record of Processing Activities (ROPA) that helps companies comply with Art.30 of the GDPR. All records are persisted in the Profile Service and are made available to SENTINEL plugins (such as GDPR CSA, DPIA and CSRA) as required. This KR is considered ~100% achieved.

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

This KR is tightly connected with KR-2.4 and is related to the delivery of an integrated IdMS. As mentioned above, the IdMS is offered as-a-service that provides a range of functionalities to the SME/ME including i) Central, EU-wide, self-service identity management, ii) Credentials and access tokens management that allow Authentication (AuthN) of the above identities, iii) Role Based Access Control (RBAC), iv) Federation with 3rd party applications, based on protocols that allow scalable expansion according to the needs of SMEs/MEs wanting to leverage SENTINEL IdMS, v) considering My Data principles, data management scheme for secure, GDPR compliant storage and access of user data, vi) Governance. Adoption and widespread utilization of the unified IdMS have been verified as part of WP6 activities, where the SENTINEL use case owners tested the system in real-world settings. KR is considered ~100%

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

Technical partners have developed from scratch as well as leveraged tried-and-tested **tools and services (22 in total)**, utilized/integrated in SENTINEL FFV final version (released in M30). A brief list of these tools is presented in the following:
The MITIGATE framework, provided by FP, and integrated with SENTINEL's FFV, is delivering a number of user-facing tools and services:
(1) The Vendor and Product Management service
(2) The asset inventory service (online ISMS for SMEs/MEs)
(3) The Vulnerability Management service
(4) The Common weaknesses management service
(5) The Threat Management service
(6) The Simulation Environment
All above MITIGATE services are integrated in SENTINEL via the
(7) CyberSecurity Risk Assessment (CSRA) SA tool
(8) GDPR Compliance Self-Assessment (GDPRCSA) developed by LIST.
(9) Data Protection Impact Assessment (DPIA), provided by STS
(10) Security Infusion (SI) is an all-in-one solution provided and supported by ITML

(11) Identity Management Service (IdMS), provided by ITML
(12) Observatory Information Exchange (supported by ITML)
(13) Observatory Knowledge Base
SENTINEL's OTM recommendations are accompanied with
(14) Open-Source software/plugins and educational or training material, curated by TSI
(15) the CyberRange, contributed by ACS
(16) receive security notifications, through the integration of Security Infusion (SI) with the SENTINEL Notification Aggregator
(17) handle and share cybersecurity incidents and data breaches, as they occur, leveraging the Incident Reporting module
(18) create and edit a data protection-oriented organisational profile, complete with a global asset profile, MITIGATE-modelled asset inventory and a complete Processing Activities data capturing model shared with the self-assessment tools
(19) record their processing activities in a permanent, immutable and auditable ROPA, thus satisfying Art. 30 of the GDPR;
(20) obtain tailor-made recommendations of measures (OTMs), software and trainings, based on thorough analysis of every aspect of their profile and processes facilitated through an intelligent synergy of SENTINEL's Recommendation Engine (RE) and Policy Drafting (PD) modules
(21) Policy Enforcement tool, integrated with each policy draft.
(22) Policy Monitoring
Further details about these tools and the respective technical works/progress are reported in D2.3, D3.3, D4.3, D5.3, D5.6. The current KR is directly related with iKPI-2.3 and it is considered 100% achieved.

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

The work completed up to M30, from setting the project's baseline (WP1), to delivering the final version of SENTINEL (WP2-WP5) has directly or indirectly contributed to this Key Result. The project's technical partners have designed, developed and deployed a total of fifteen (15) distinct tools and services for cybersecurity, personal data protection and GDPR compliance, and integrated them with SENTINEL. These tools and services are:

1. SME profiling
2. Cyber asset inventorying
3. Personal data processing activities (PA) capturing
4. GDPR compliant recording of PAs (ROPA)
5. GDPR compliance self-assessment (GDPRCSA)
6. Data protection impact assessment (DPIA)
7. Cybersecurity risk assessment (CSRRA)
8. Policy recommendations for OTMs, software and training material
9. Policy enforcement monitoring: tracking the implementation status of OTMs
10. Cyber Range simulations with realistic SME scenarios
11. Identity management system (IdMS)
12. Cyber incident reporting and handling
13. Receiving security notifications
14. Observatory Knowledge Base (KB)
15. Observatory aggregation of CS and PDP sources and data feeds

The period leading to M30, including the final execution of the SENTINEL demonstrations has allowed us to measure this KR both qualitatively and quantitatively, since the tools and services above have participate in all of the use cases of the final release of SENTINEL. Collectively, considering progress and completion aspects for the capabilities, tools and services in the listing above, we have recoded an overall average progress of 100% for the KR (an assessed value of 15 vs a baseline value of 10, also considering individual components' completion rate).

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

At the FFV phase, Recommendation Engine (RE) has been continuously updated and enriched to further increase its accuracy aiming to significantly advance SENTINEL services in privacy-aware environments

for SMEs/MEs. Currently SENTINEL's Common Service has been enriched with over 50 open-source tools and around 120 training courses. Cyber assets in the inventory now support asset locality and ownership. This makes the RE inputs and outputs even more dynamic and tailored to end-user needs. The above have been reported in D3.3 "The SENTINEL digital core: Final Product".

KR-3.4: Accuracy and efficiency of the SENTINEL data privacy compliance recommendation engine at least 70%. Owner: **ITML**

The purpose of the SENTINEL recommendations is to provide a list of recommended measures, plugins and trainings, to assist the organisation to address potential shortcomings and vulnerabilities in the realm of data protection and cybersecurity protection. For the MVP (D3.1), and FFV versions the Recommendation Engine (RE) leverages a simple and pre-specified hard-coded rule to map Organisational and Technical Measures (OTMs) that correspond to a given risk assessment level with a list of plugins, trainings and other optional capabilities. Those versions have been measured with respect to i) responsiveness of about 50ms and ii) 100% availability. In the final version of the RE (D3.3) a rule-based mechanism is implemented where more complex rules need to be handled, thus latency in the responsiveness of the system is expected to slightly increase.

KR-4.2: Delivery of three (3) integrated versions of the SENTINEL framework. Owner: **INTRA**

The MVP constituted the first integrated version of the SENTINEL framework and was delivered in M12 and reported in D5.4, the FFV was delivered in M18 and reported in D5.5 while the final platform release delivered in M30 and reported in D5.6. This KR is 100% achieved.

KR-4.5: Construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs. Owner: **AEGIS**

Several meetings have been carried out to define and implement the User Interface (UI) of the SENTINEL platform, namely MySentinel. As part of these meetings, updated versions for the mock ups have been presented to the consortium alongside an initial version for the User Journey. Continuous work has been carried out on the UI since the start of the project. By M12, the MySentinel dashboard included links to components that were incorporated in the MVP, as well as the relevant pages. Organization Profile, Processing Activities, Contact Persons, Assets, Self-Assessment tools, Policy Recommendations and a Threat Intelligence Platform (TIP) comprised the modules offered to the end-user by the SENTINEL platform in the MVP phase (more details in D5.1).

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

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

By M30, comprehensive work has been carried out in order to refine and enrich the content of the UI by constantly engaging and closely collaborating with end-users (under WP6), incorporating their feedback and implementing a UI/UX which offers true usability. Additionally, we have made several technical adaptations required in the communication of the UI with all modules as the work progressed. This effort resulted in the final version of the MySentinel UI and is documented in the last deliverable of the series, namely D5.3. This KR is 100% complete.

7. Conclusion and next steps

This report presents the work conducted in the frame of WP6 “Real-life experiment evaluations: SENTINEL pilots” mainly for Tasks “T6.2 – Validating SENTINEL offerings to SMEs and MMs: Test cases in the fields of genomics and social care”, “T6.3 - Open access to the SENTINEL platform for validation and evaluation through Digital Innovation Hubs” and “T6.4 - Evaluation and impact analysis”.

It elaborates on the SENTINEL FFV Demonstration and Validation phases well-aligned with the SENTINEL technical development activities conducted in between M19-M30. Furthermore, it illustrates the work conducted with respect to i) the deployment of the SENTINEL test cases in the fields of genomics and social care, ii) the development of the Persona Based Approach by profiling our end-users and creating personas, iii) the demonstration of the Full-Featured Version (FFV) of the SENTINEL platform, iv) the trials execution and output collection and feedback analysis.

The end-user feedback gained from the three SENTINEL Pilots (i.e., CG Pilot, TIG Pilot, DIH Pilot) helped to build the SENTINEL personas and were also considered in the technical enhancements of the SENTINEL UI component reported in “D5.3 - The SENTINEL visualisation and UI component - final version”.

The future work envisioned in WP6 is to strongly collaborate with additional SMEs/MEs to test the SENTINEL integrated solution final version and provide feedback to formulate the project’s impact analysis and carry out an overall assessment and evaluation of the SENTINEL platform as part of “T6.4 - Evaluation and impact analysis”. This will be accompanied with a series of actions planned for the upcoming period (until M36), including KRs/KPIs assessment for each demonstrator both in operational (cost, service levels, etc.) and technical terms (performance of solution), organization of final workshop by engaging additional SMEs/MEs. The respective work will be documented in deliverable “D6.3- Assessment report and impact analysis” (M36).

References

[1] Deliverable D1.3 (2021), “The SENTINEL Experimentation Protocol”, SENTINEL EU H2020 Project.
[2] Deliverable D6.1 (2022), “SENTINEL Demonstration - initial execution and evaluation”, SENTINEL EU H2020 Project.
[3] Deliverable D5.3 (2023), “The SENTINEL visualisation and UI component - final version”, SENTINEL EU H2020 Project.
[4] Karolita, D., McIntosh, J., et. al. (2023), Use of personas in Requirements Engineering: A systematic mapping study, Information and Software Technology, Volume 162, 2023, 107264, ISSN 0950-5849, https://doi.org/10.1016/j.infsof.2023.107264
[5] Ferreira, B., Williamson, S. et al. (2018), Technique for representing requirements using personas: a controlled experiment, IET Software, 12(3), June 2018, pp. 280 – 290
[6] ISO/IEC 25010: 2011 “Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models”. Online available: https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en
[7] European Parliament and Council of the European Union. Regulation (EU) 2016/679 (GDPR) Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EL
[8] ISO/IEC 33001:2015: ISO - ISO/IEC 33001:2015 - Information technology — Process assessment — Concepts and terminology
[9] CVE MITRE. Online available: https://cve.mitre.org/

Appendices

Appendix -I: SENTINEL User Evaluation Questionnaire

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

Section 1 of 9

SENTINEL User Evaluation Questionnaire

Dear Sir/Madam,

thank you for your participation in the SENTINEL Full Featured Version (FFV) evaluation process!

Introduction

The objective of the "SENTINEL User Evaluation Questionnaire" is to give the opportunity SMEs/MEs end-users to communicate their feedback and comments regarding (a) the overall functionality of the SENTINEL FFV and (b) the way that the SENTINEL FFV addresses the specific Cybersecurity and Personal Data Protection requirements of the different processing activities involved in SMEs/MEs daily business operations.

The questionnaire aims to make everything quantifiable and measurable regarding the overall quality of the SENTINEL platform, e.g., identify usability, visualisation or performance issues, and determine the participant's satisfaction towards the SENTINEL platform according to specific variables and metrics identified from the project's consortium, which reflect the project's specific Key Performance Indicators (KPIs) and Key Results (KRs).

The results of this evaluation will be considered towards the development of the SENTINEL final version.

Privacy and confidentiality statement

With your participation in this questionnaire, you agree to the processing of your personal information, that is, company, position and contact details, by the SENTINEL consortium to study and extract anonymous information regarding user satisfaction. The SENTINEL consortium—specifically all the organisations involved in gathering, processing and analysing end-user needs— fully understands the sensitive nature of the subject and will not include any information that is not suitable for the public domain. At the same time, all respondents' personal details will remain anonymous and 'firewalled'. The data will be anonymized and aggregated to keep them confidential.

Participation in this study is voluntary. If you choose to participate, you can nonetheless end with this questionnaire at any time without being required to provide any explanation. Should you wish to withdraw your consent regarding the processing of your personal data, you can contact Dr. Siranush Akarmazyan [siranush@itml.gr].

The SENTINEL project

SENTINEL is a European project, funded by the EU H2020 Research and Innovation program under grant agreement No 101021659. SENTINEL's main offerings rely on:

(i) populating each SME's profile, including capturing their Personal Data Processing Activities and cyber assets, with which to identify the SME requirements towards improving privacy and achieving GDPR compliance;

(ii) bridging the gap between cybersecurity and personal data protection through the provision of evidence-based GDPR compliance;

Section 2 of 9

User Details

Description (optional)

1. Organisation Name: *

Short answer text

2. Department Name: *

Short answer text

3. What is your current position in the organisation? *

Short answer text

4. What is your area of expertise? *

- ○ IT/Information Security
- ○ Personal Data Protection
- ○ Technology and Engineering
- ○ Human Resource Management
- ○ Production
- ○ Sales & Marketing
- ○ Accounting and Finance
- ○ Health & Social Care
- ○ Other...

5. Please identify your level of expertise regarding cybersecurity.

- ○ Beginner
- ○ Intermediate
- ○ Expert

6. Please identify your level of expertise regarding personal data protection and EU GDPR compliance regulation? *

- ○ Beginner
- ○ Intermediate
- ○ Expert

7. Are you currently involved in performing or assessing cybersecurity, privacy or personal data protection processes in your organisation? *

- ○ Yes
- ○ No

8. If yes, please specify your involvement and related tasks.

Long answer text

9. Does your organisation employ any tools or services for privacy assessment to estimate and/or support its GDPR compliance? *

- ○ Yes, internal (software tool)
- ○ Yes, external services (consultants)
- ○ Yes, both (software tool and consultancy)
- ○ No to my knowledge

10. If yes, what are your annual expenses with respect to GDPR compliance, approximately?

Please note: Consider including in your answer costs for implementation of both Organisational and Technical Measures (OTMs) as well as costs for maintenance of GDPR compliance, costs for technical solutions (e.g. cloud services or CRM, HR dedicated to GDPR, training costs, consultancy fees, etc.)

- ○ 0 € (Free and open-source services)
- ○ 1-999 €
- ○ 1,000-9,999 €
- ○ 10,000-50,000 €
- ○ >50,000 €
- ○ Other...

11. If no, does your company plan to invest on such tools/services in the future?

- ○ Yes, within the next two years
- ○ No to my knowledge
- ○ Other...

12. If you have selected "Yes, within the next two years" in Q11, please provide an approximate cost you are willing to pay annually.

Short answer text

13. If you perform GDPR compliance, how frequently do you undertake compliance audits?

Short answer text

14. Please specify the license type your organisation adopts for GDPR compliance tools/services. *

15. Please summarise any specific concerns you have about cybersecurity and personal data protection in your organisation. *

Short answer text

16. Do you believe that the SENTINEL platform can help to resolve your concerns? *

Short answer text

After section 2 Continue to next section

Section 3 of 9

Experiment Details

Please provide some information regarding the processing activity (PA) you have used to test SENTINEL.

What processing activity did you use? *

- I used one of the pre-filled processing activities («Marketing activities & Communication», «Recruitment ...
- I created my own processing activity by following the instructions provided in the SENTINEL platform "H...
- Both of the above

If you created your own processing activity, please provide its name.

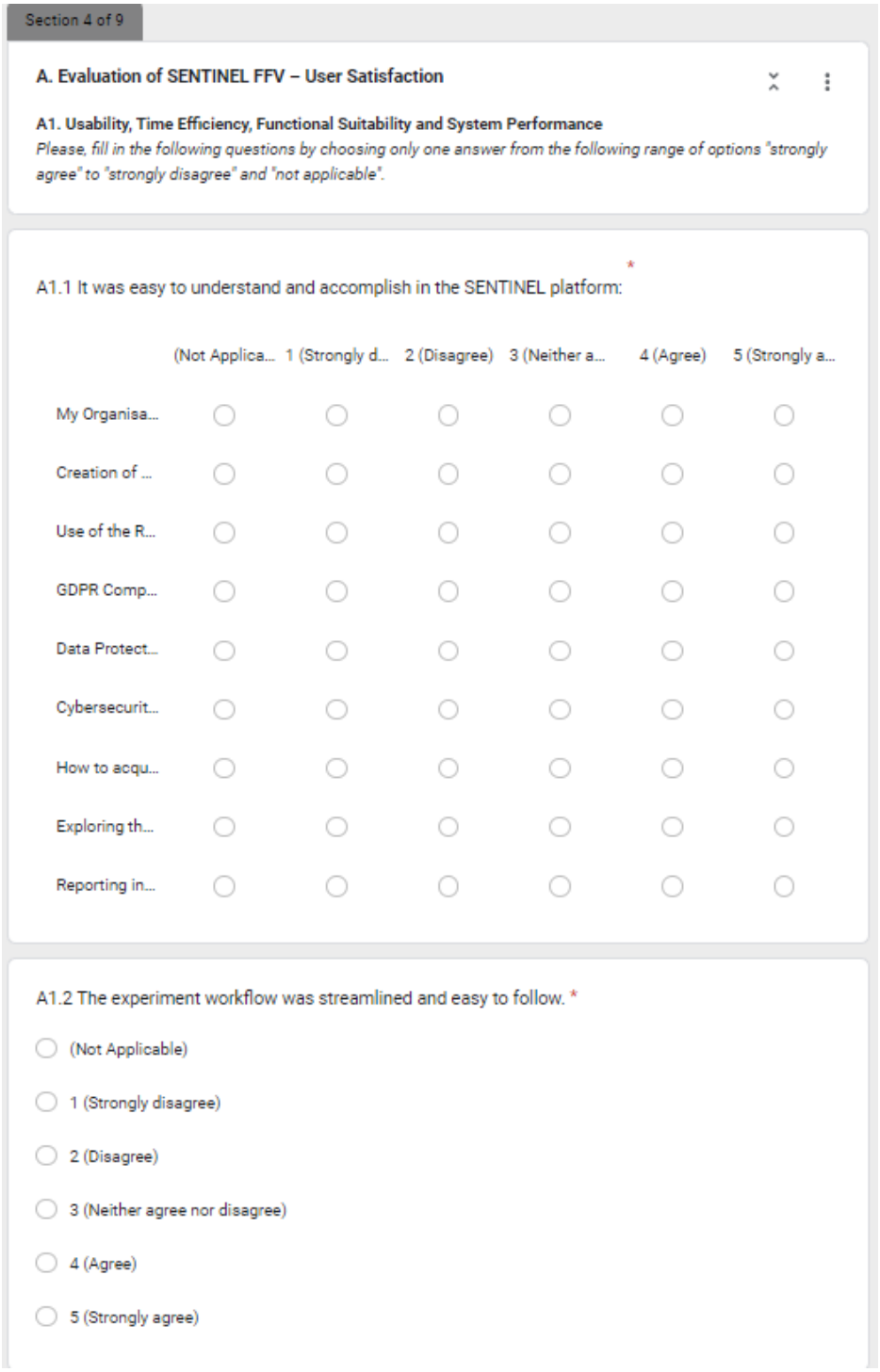
Short answer text

If you created your own processing activity, please provide a brief description of it.

Long answer text

If you created your own processing activity, what type of data it involved?

- Customer



Section 4 of 9

A. Evaluation of SENTINEL FFV – User Satisfaction

A1. Usability, Time Efficiency, Functional Suitability and System Performance

Please, fill in the following questions by choosing only one answer from the following range of options "strongly agree" to "strongly disagree" and "not applicable".

A1.1 It was easy to understand and accomplish in the SENTINEL platform: *

	(Not Applica...	1 (Strongly d...	2 (Disagree)	3 (Neither a...	4 (Agree)	5 (Strongly a...
My Organisa...	○	○	○	○	○	○
Creation of ...	○	○	○	○	○	○
Use of the R...	○	○	○	○	○	○
GDPR Comp...	○	○	○	○	○	○
Data Protect...	○	○	○	○	○	○
Cybersecurit...	○	○	○	○	○	○
How to acqu...	○	○	○	○	○	○
Exploring th...	○	○	○	○	○	○
Reporting in...	○	○	○	○	○	○

A1.2 The experiment workflow was streamlined and easy to follow. *

- ○ (Not Applicable)
- ○ 1 (Strongly disagree)
- ○ 2 (Disagree)
- ○ 3 (Neither agree nor disagree)
- ○ 4 (Agree)
- ○ 5 (Strongly agree)

A1.3 SENTINEL provides efficient guidance and help menu to allow the user to conduct privacy assessments (GDPR Compliance Self-Assessment and Data Protection Impact Assessment) on the organisation's Processing Activities even if he/she is a beginner on privacy and personal data protection topics. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A1.4 SENTINEL Recommendations to SMEs/MEs for undertaking technical and organisational measures (Policy Draft) to increase their level of security and GDPR compliance are described accurately and clearly. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A1.5 It was easy to understand the structure and logic of the SENTINEL Dashboard Menu and easy to use. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A1.6 The SENTINEL platform provides helpful and sufficient visualization capabilities and interactive control of the working process as well as the reports, the dashboard help menu and tooltips (e.g. helpful shortcuts from one function to another). *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A1.7 I am satisfied with the performance of the SENTINEL system in terms of speed when: *

	(Not Applica...	1(Strongly di...	2 (Disagree)	3 (Neither a...	4 (Agree)	5 (Strongly a...
Filling in My ...	○	○	○	○	○	○
Creating a P...	○	○	○	○	○	○
Using the R...	○	○	○	○	○	○
Executing G...	○	○	○	○	○	○
Executing D...	○	○	○	○	○	○
Executing C...	○	○	○	○	○	○
Acquiring po...	○	○	○	○	○	○
Exploring th...	○	○	○	○	○	○
Reporting in...	○	○	○	○	○	○

A1.8 In addition to Q A1.7, what was the approx. time required to complete the experiment's workflow? *

- (Not Applicable)
- less than or equal to 15 min

A1.9 The SENTINEL platform gave error messages that clearly told me how to fix problems. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A1.10 Please suggest how we could improve the SENTINEL platform's functionalities.

Long answer text

A. Evaluation of SENTINEL FFV – User Satisfaction

A2. SENTINEL User Interface/User Experience (UI/UX)

Please, fill in the following questions by choosing only one answer from the following range of options "strongly agree" to "strongly disagree" and "not applicable".

A2.1 The characters on the screens are easy to read. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A2.2 The language used in SENTINEL is comprehensive. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A2.3 The information (i.e. on-screen messages, and other documentation and tooltips) provided with the dashboard is accurate and clear. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)

A2.4 The organization of information on the SENTINEL screens is clear and user-friendly. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A2.5 SENTINEL has clearly marked way-finding buttons (exit, back, next page, etc.) *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A2.6 The use of terms throughout SENTINEL is consistent. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A2.7 The position of messages on the screens is proper. *

A2.8 The different screens of SENTINEL are cohesive in look-and-feel. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A2.9 The interface of SENTINEL is pleasant. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A2.10 SENTINEL templates helped me to identify and record my organisation's processing activities. *

- (Not Applicable)
- 1 (Stronlgly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A2.11 SENTINEL overall provides all the functions and capabilities I expect to have for assessing privacy (GDPR compliance and data protection Impact assessment) of my *

A3. SENTINEL's CyberRange Gaming

Please, fill in the following questions by choosing only one answer from the following range of options "strongly agree" to "strongly disagree" and "not applicable".

A3.1 It was easy to understand and test the CyberRange Gaming. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A3.2 The CyberRange Gaming has helped me to explore different types of threats and attacks related to data storage and accessibility. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A3.3 The CyberRange Gaming has helped me to acquire good practices to better protect my data. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)

A3.4 The CyberRange Gaming has helped me to detect, analyse and better understand vulnerabilities on ICT assets. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A3.5 Please suggest how to improve the CyberRange Gaming.

Long answer text

A4. SENTINEL Results, Security, Quality, Personal Data Protection and Compliance

Please report on the results that were obtained during the experiment. Please provide your response in a free text (Indicate either "number, text") or provide only one answer from the following range of options "strongly agree" to "strongly disagree" and "not applicable".

A4.1 Do you think that the SENTINEL measures/recommendations can increase GDPR compliance of your Processing Activities in an efficient manner. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A4.2 Do you think that the SENTINEL measures/recommendations can assure privacy of related data? *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A4.3 Did you find any recomendations/suggested tools/techniques that can be utilised to increase the security and privacy of your Processing Activities? *

Short answer text

A4.4 Do you think that SENTINEL Cybersecurity simulation environment has helped you to identify risks/threats to the registered assets? *

Short answer text

A4.5 Do you think that SENTINEL measures/recommendations can mitigate risks/threats identified within your experiment? *

Short answer text

A4.6 Do you think that the SENTINEL Cybersecurity simulation environment has helped you to identify possible attack scenarios? *

Short answer text

A4.7 Can privacy incidents be prevented by implementing SENTINEL recommendations? *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A6. SENTINEL Business Performance

Please, fill in the following questions by choosing only one answer from the following range of options "strongly agree" to "strongly disagree" and "not applicable" .

A6.1 The SENTINEL services can help address challenges I face in my organisation with respect to privacy and cybersecurity. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A6.2 I did not face any interruptions while using the SENTINEL platform. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A6.3 SENTINEL can be used for all processing activities and assets used for data storage and accessibility in my organisation. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)

A6.4 The measures recommended by SENTINEL can improve *

	(Not Applica...	1 (Strongly d...	2 (Disagree)	3 (Neither a...	4 (Agree)	5 (Strongly a...
Cybersecurit...	○	○	○	○	○	○
Implementat...	○	○	○	○	○	○
Security of i...	○	○	○	○	○	○
Maintenanc...	○	○	○	○	○	○

A6.5 I find that the SENTINEL platform is easy to learn. *

- ○ (Not Applicable)
- ○ 1 (Strongly disagree)
- ○ 2 (Disagree)
- ○ 3 (Neither agree nor disagree)
- ○ 4 (Agree)
- ○ 5 (Strongly agree)

A6.6 I am satisfied with the time needed to complete the privacy assessment (A GDPR Compliance Self-Assessment and Data Protection Impact Assessment) and receive recommendations. *

- ○ (Not Applicable)
- ○ 1 (Strongly disagree)
- ○ 2 (Disagree)
- ○ 3 (Neither agree nor disagree)
- ○ 4 (Agree)
- ○ 5 (Strongly agree)

A6.7 I think that SENTINEL simplifies privacy assessment (GDPR Compliance Self-Assessment and Data Protection Impact Assessment) comparing to the tools/services we are currently using. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A6.8 I think that SENTINEL simplifies cybersecurity risk analysis comparing to the tools/services we are currently using. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A6.9 The measures recommended by SENTINEL will improve the effectiveness of my organisation regarding cybersecurity and personal data protection processes completion. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A6.10 Using SENTINEL will not necessitate additional human and/or financial resources (e.g. hiring external cybersecurity analysts and privacy experts) from my organisation. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A6.11 Using SENTINEL has helped me understand my organisations' GDPR compliance requirements. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

A6.12 Using SENTINEL can help me form my organisations' cybersecurity and personal data protection strategy. *

- (Not Applicable)
- 1 (Strongly disagree)
- 2 (Disagree)
- 3 (Neither agree nor disagree)
- 4 (Agree)
- 5 (Strongly agree)

B. Evaluation of the SENTINEL platform – Express your opinion

Please, answer the following questions by providing your feedback in free text.

B1. How would you describe the quality of SENTINEL privacy assessments (GDPR Compliance Self-Assessment and Data Protection Impact Assessment) results in general? *

Long answer text

B2. How would you describe the quality of SENTINEL cybersecurity risk analysis? *

Long answer text

B3. Please, specify any issues (e.g. bugs, content, layout, design, errors, etc.) you faced while using the platform to test the functionalities of the SENTINEL platform. *

Long answer text

B4. Please, describe the aspects you find most positive concerning the functionalities of the SENTINEL platform. *

Long answer text

B5. Based on your needs, please describe any additional services/capabilities that you would like to see in the SENTINEL platform. *

Long answer text

B6. Please provide further comments/suggestions for improvements after your experience with SENTINEL. *

Long answer text

Thank You for Completing Our Questionnaire!

We truly value the information you have provided.

Your responses are vital for the success of the SENTINEL EU H2020 project.

Appendix -II: SENTINEL End-User Instructions

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

3rd Pilot on Digital Innovation Hubs (DIHs)

SMEs Trial Execution and Evaluation

End-User Instructions

September 2023

Dear Sir/Madam,

thank you for your participation in the SENTINEL 3rd Pilot trial execution and evaluation processes! The SENTINEL project kindly invites external SMEs to try and validate the Full Featured Version (FFV) of the SENTINEL platform from a twofold perspective:

(i) to test the available functionalities of SENTINEL FFV under real-life operation scenarios and provide feedback considering their personal experience gained after performing the trial along with other validation criteria, such as usability, performance, user satisfaction, user interface (UI), speed, flexibility, quality, efficiency;

(ii) to test the way that SENTINEL FFV addresses privacy, personal data protection and cybersecurity requirements of different processing activities utilised by SMEs in their daily business

To execute the trials, you will need to visit the SENTINEL platform via the following link (https://platform.sentinel-project.eu/) and implement at least one pilot experiment, as indicated in the current instructions.

After completing the trial in the SENTINEL platform, please fill in the online "SENTINEL User Evaluation Questionnaire" which can be accessed here. The results of this evaluation will be considered in the ongoing technical development works of the SENTINEL platform.

***NOTE:** Before starting to execute the trial, please bear in mind to track the time needed to test the SENTINEL platform for each pilot experiment, since you may need this information while filling the questionnaire.*

The SENTINEL project

SENTINEL is a European project, funded by the EU H2020 Research and Innovation program under grant agreement No 101021659. SENTINEL's main offerings rely on:

(i) populating each SME's profile, including capturing their Personal Data Processing Activities and cyber assets to identify the SME requirements towards improving privacy and achieving GDPR compliance;

(ii) bridging the gap between cybersecurity and personal data protection through the provision of evidence-based GDPR compliance;

(iii) cutting costs through automation by offering recommendations and a better overall understanding of the measures (OTMs) required, backed up with cybersecurity, privacy and related policy & compliance monitoring.

For further information about the project, please visit our website: https://sentinel-project.eu/.

List of Abbreviations

Abbreviation	Description
DIH	Digital Innovation Hubs
GDPR CSA	GDPR Compliance Self-Assessment
CSRA	Cybersecurity Risk Assessment
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
FFV	Full Featured Version
IOC	Indicators of Compromise
MISP	Malware Information Sharing Platform
OTM	Organisational and Technical Measure
PA	Processing Activity
PDP	Personal Data Protection
ROPA	Registry of Processing Activities
UI	User Interface
UX	User Experience

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

Contents

SENTINEL Experiment Workflow

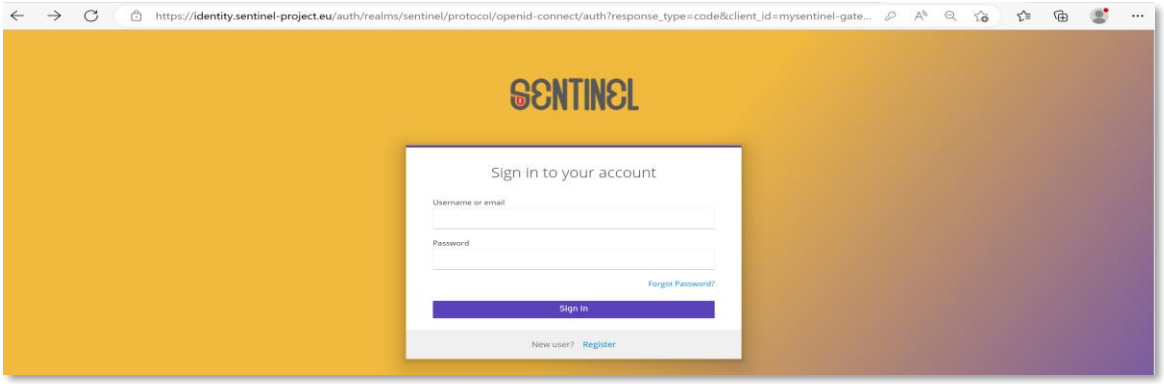
The SENTINEL pilot experiment can be accomplished by entering the SENTINEL platform and performing the **pipeline of actions.**

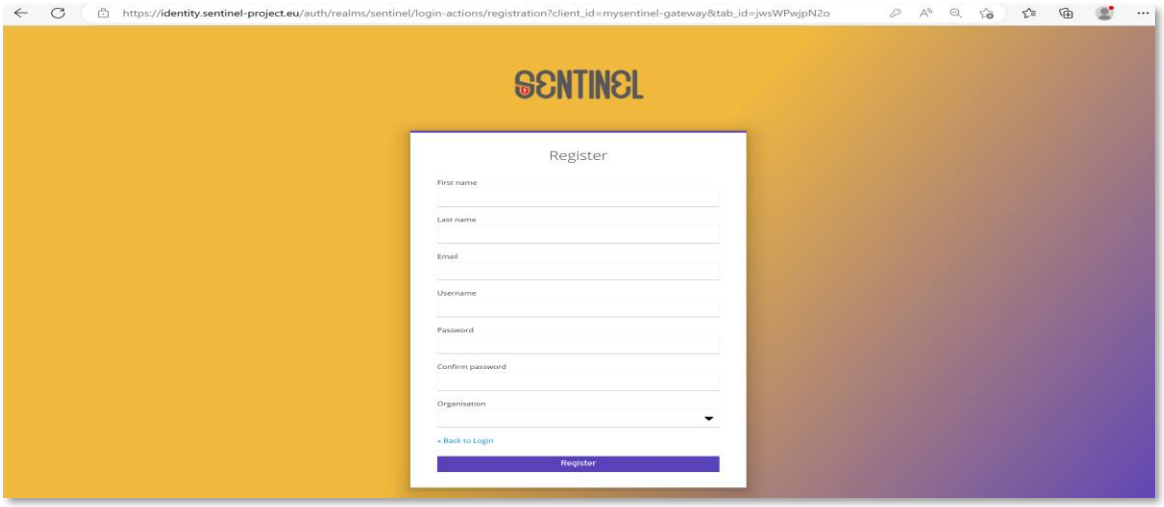
The following sections present detailed instructions for executing this linear pipeline of actions in the SENTINEL platform analysed per individual action.

As an initial step, to utilise the SENTINEL functionalities, you may register/sign in the SENTINEL platform.

0. Register/Sign in the SENTINEL platform

Before performing the SENTINEL experiment, registration is needed by the company representatives accessing the SENTINEL platform for the first time and signing in after creating a user account. The company representative accesses the SENTINEL platform though the link https://platform.sentinel-project.eu and creates an account by clicking the “Register” button, as shown below:





Upon successful registration to the SENTINEL platform, the SENTINEL user visits the SENTINEL platform through the link https://platform.sentinel-project.eu and signs in.

Create a complete profile for your organisation

To execute this action, the following items rely in the current action must be filled in the SENTINEL platform sequentially, as presented hereunder:

1.1 Org. Basic data

1.2 Org. Contacts

1.2 Org. Generic assets profile

1.3 Org. Assets inventory

1.4 Org. GDPR compliance

1.5 Org. Measures

Organisation Profiling

Upon successful sign-in, the SENTINEL user creates the profile of the organization by accessing the category “My Organisation” from the SENTINEL Dashboard menu and filling in all information required about the organization:

1.1 Org. Basic data

Basic organisation data (Organisation/Company name, sector, country, size)

Procedure

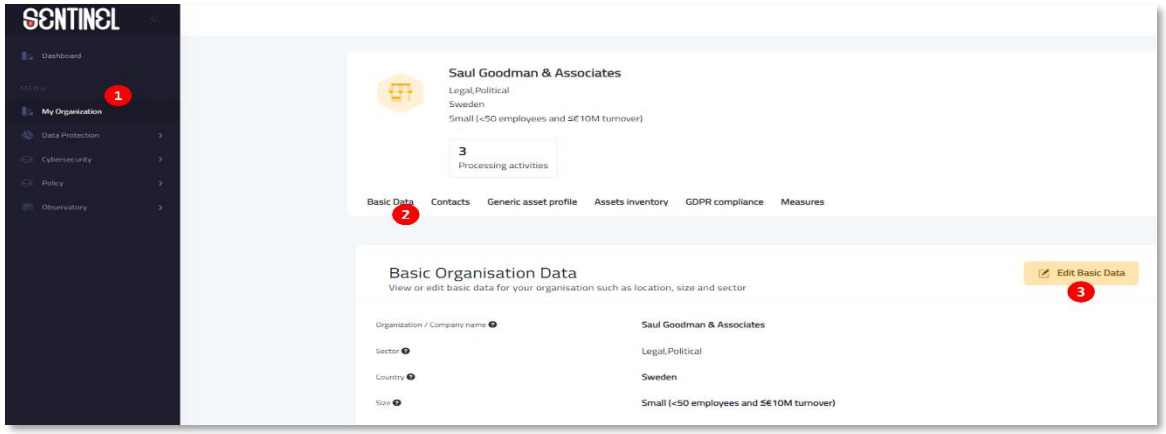
Click "My Organization" on the Main Menu

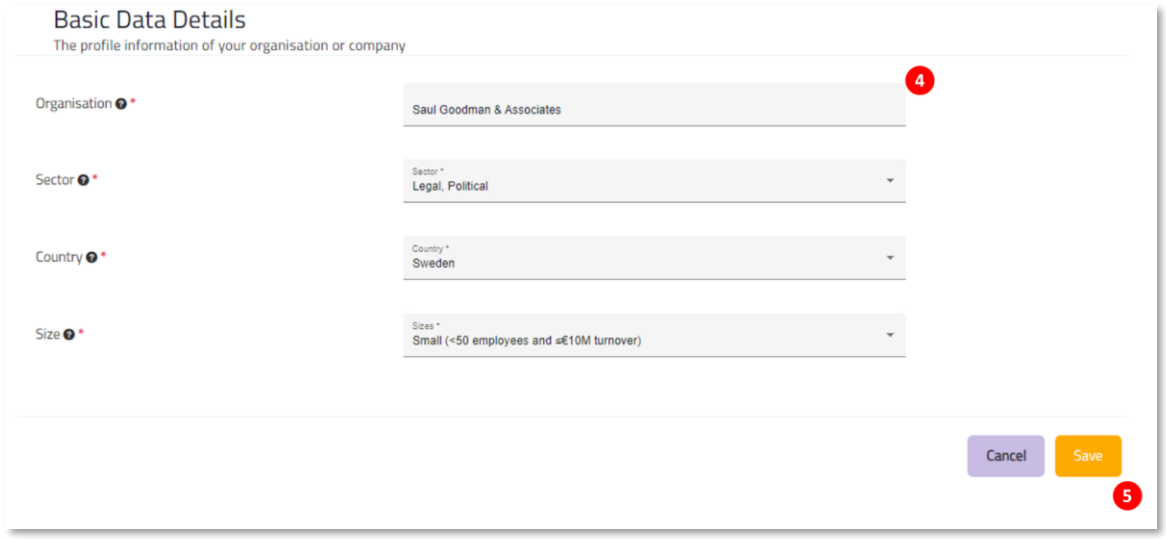
Click "Basic Data" tab

Click or tap: “Edit Basic Data” button.

Once clicked or tapped, you will be able to enter the required information. If you are unsure of what to complete, you may need to seek advice from a senior colleague.

Once you have entered the required information, click or tap: “Save”.





1.2 Org. Contacts

Details of contact persons responsible for the protection of personal data in this organization

Procedure

Click "My Organization" on the Main Menu

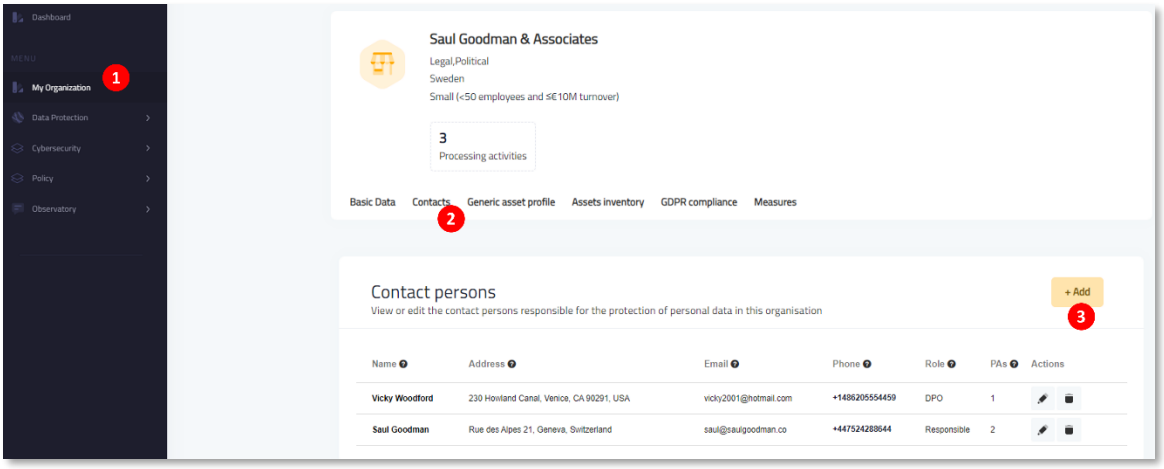
Click "Contacts" tab

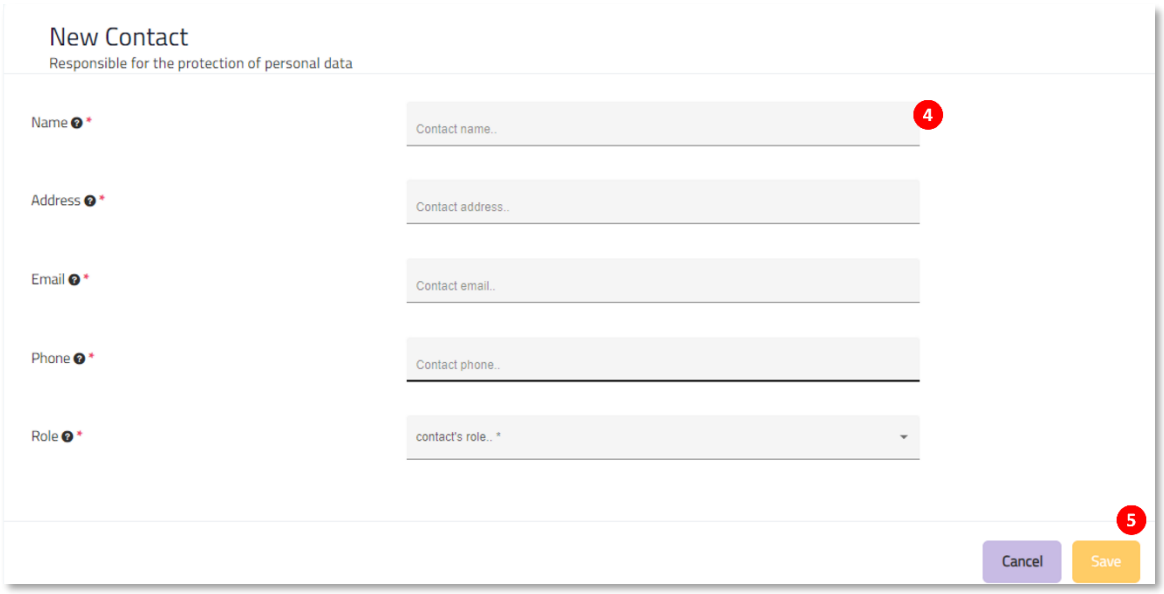
Click “Add” button.

Fill in Name, Address, Email, Phone

Select contact’s role from drop-down list

Click save





1.3 Org. Generic assets profile:

Generic (organization-wide) asset profile: asset ownership (owned/not owned), asset deployment model [locality] (on-premises/cloud/hybrid)

Procedure

Click "My Organization" on the Main Menu

Click "Generic Asset profile" tab

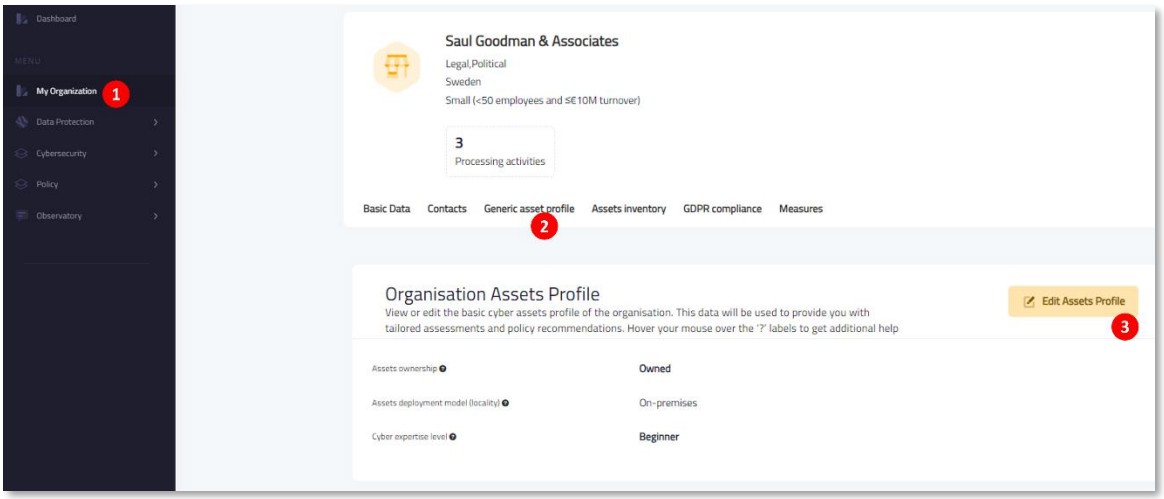
Click “Edit Assets Profile”

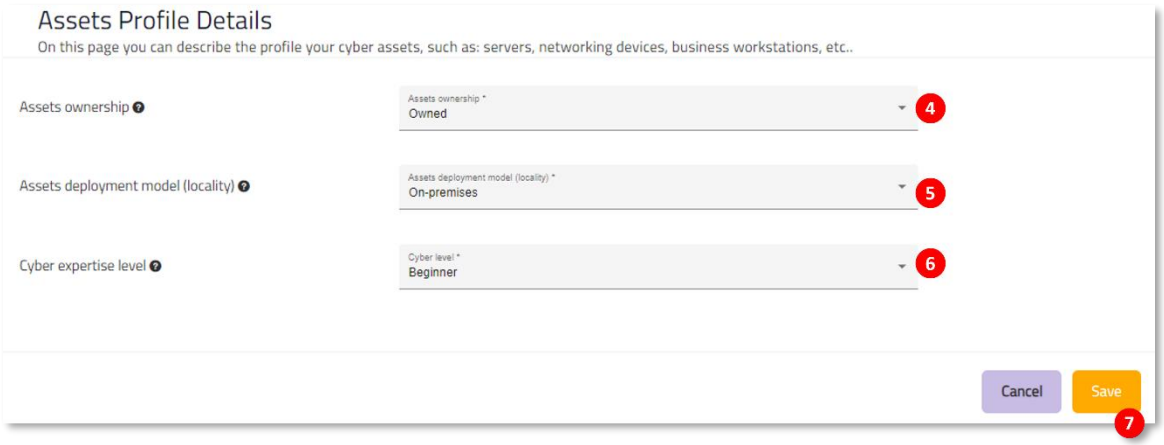
Define your Assets ownership, as owned or not owned)

Define your Assets locality, as On-premises, Cloud or Hybrid.

Identify your Cyber expertise level in three grades: Beginner, Intermediate or Expert.

Click Save





1.4 Org. Assets Inventor:

Asset Inventory. Creates a detailed asset inventory of individual asset profiles, including relationships with other assets, PAs and OTMs

Procedure

Click "My Organization" in the Main Menu

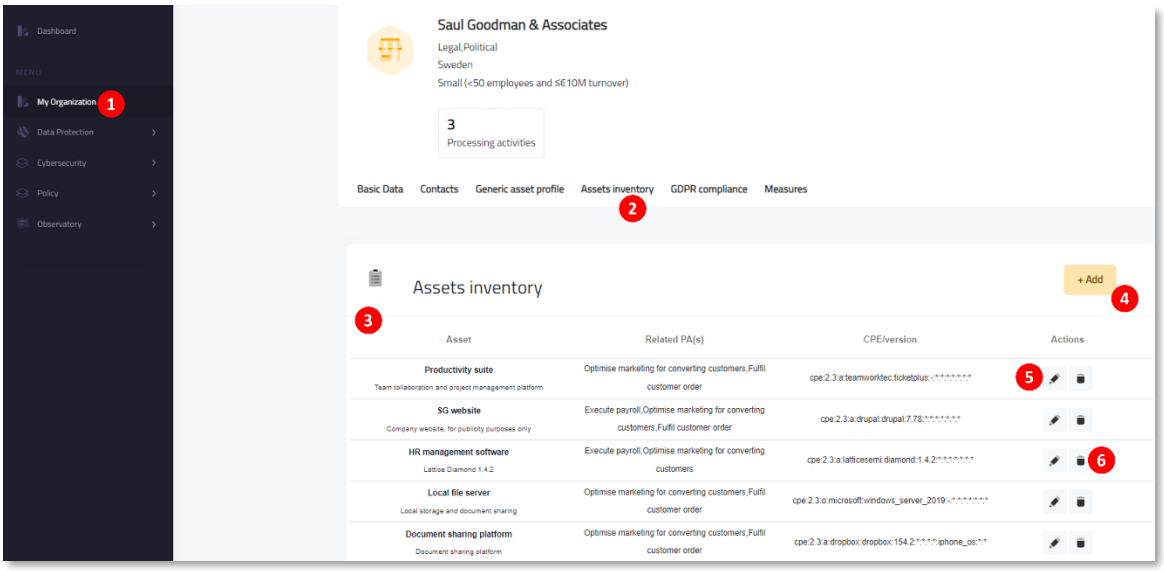
Click the “Assets Inventory” tab from the available options appeared horizontally

View the list of existing assets (in any)

Click on the “+ Add” button in order to create a new asset for the organization. (for more details see “Create new organization asset” sub-section)

Select a preferred asset from the list and click on the “Pencil” icon if you want to edit an existing asset

Select a preferred asset from the list and click on the “Garbage” icon if you want to remove an existing asset from your organization



Create new organization asset (by clicking the “+ Add” button in the Assets Inventory section, described above).

Complete the identity profile of the new asset by giving a name, providing a description, specifying the ownership (owned - not owned) and the locality of the asset (on-premise, cloud, or hybrid)

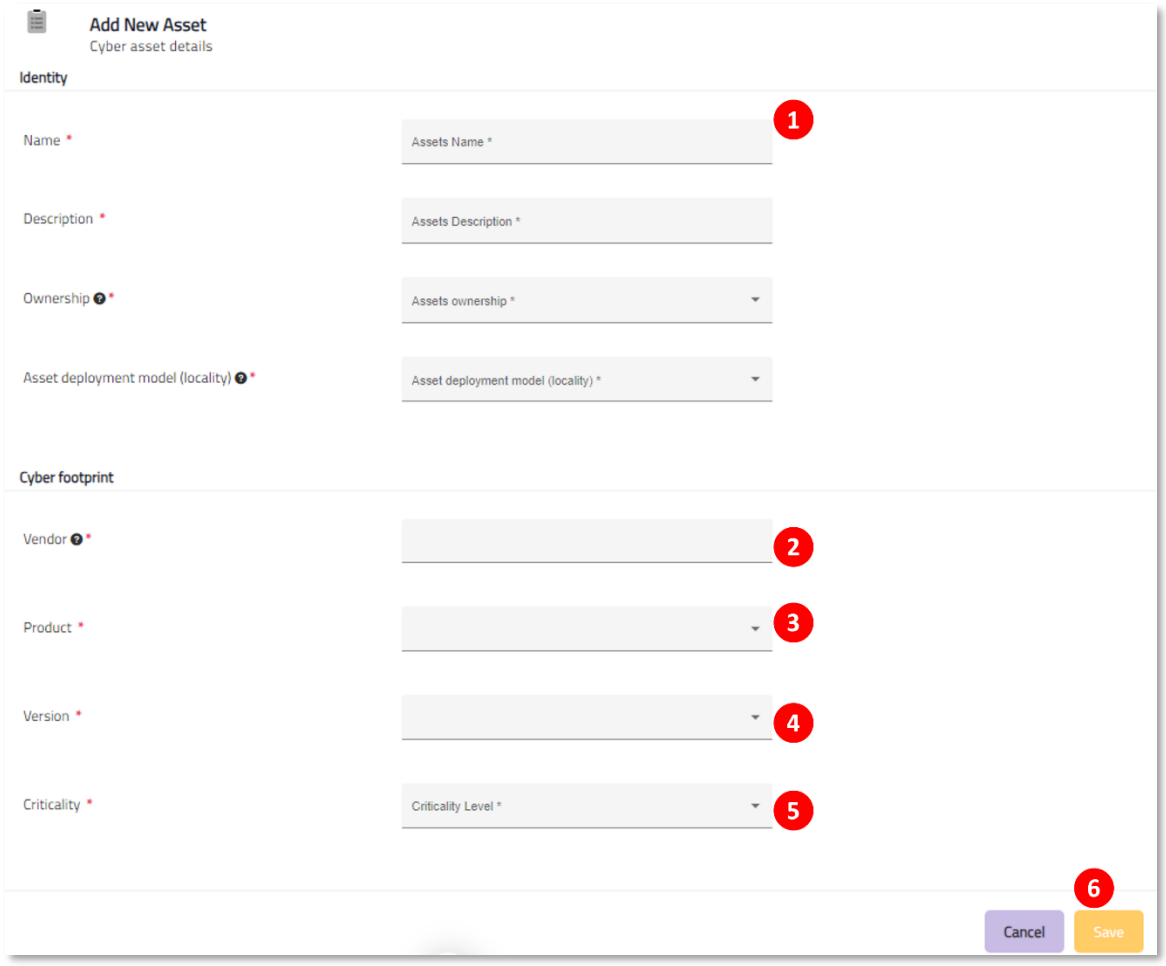
Select the vendor of your asset by typing the name of the vendor and selecting from the list its proper name

Select the specific product by typing and/or selecting from the list of available products for the preferred vendor (see previous step)

Specify the exact version from the list of available versions for the product selected in the previous step

Provide the criticality of your asset in terms of business value for your organization.

Complete the process by clicking on the “Save” button



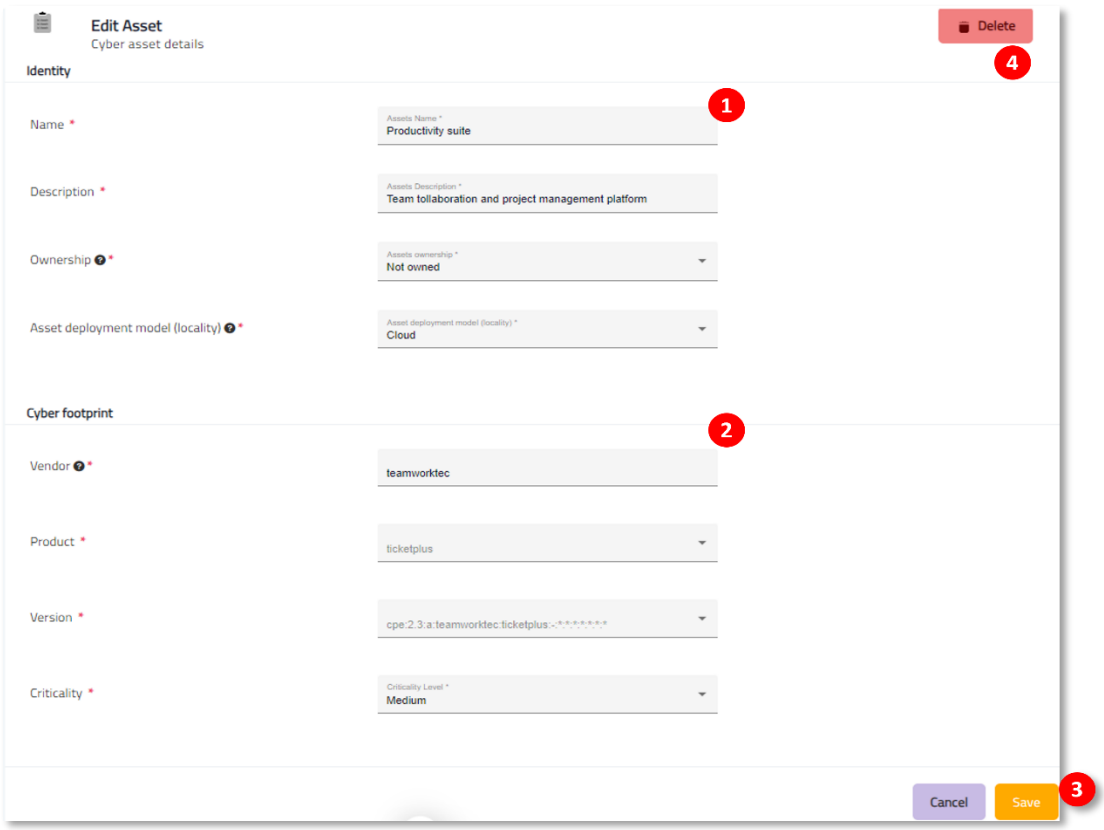
Edit the details of an existing asset, or delete it, from your assets inventory (by selecting a preferred asset from the Assets Inventory section, described above)

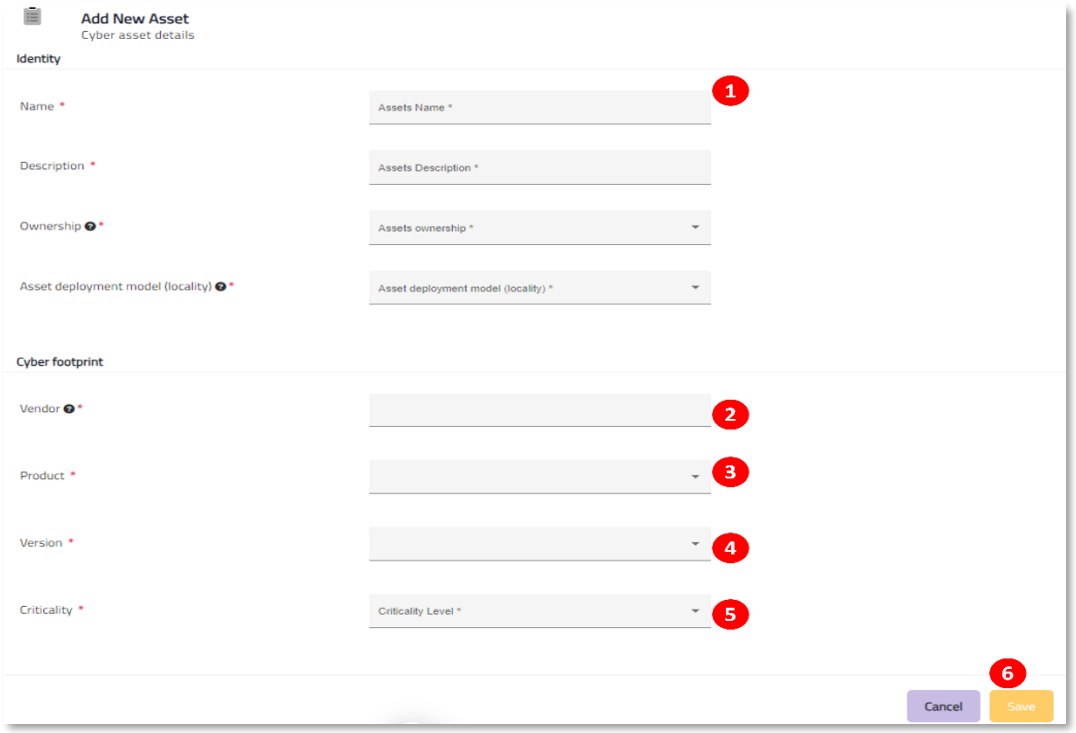
Edit the identity profile details of your preferred asset

Edit the cyber footprint of your preferred asset

Click on the “Save” button in order to save changes

(Alternatively) Click on the “Delete” button to remove the selected asset from your inventory


Edit Asset
Cyber asset details
Delete
4
Identity
Name *
1
Assets Name *
Productivity suite
Description *
Assets Description *
Team collaboration and project management platform
Ownership *
Assets ownership *
Not owned
Asset deployment model (locality) *
Asset deployment model (locality) *
Cloud
Cyber footprint
2
Vendor *
teamworktec
Product *
ticketplus
Version *
cpe:2.3:a:teamworktec:ticketplus:-:*:*:*:*:*:*:*
Criticality *
Criticality Level *
Medium
Cancel
Save
3


Add New Asset
Cyber asset details
Identity
Name *
1
Assets Name *
Description *
Assets Description *
Ownership *
Assets ownership *
Asset deployment model (locality) *
Asset deployment model (locality) *
Cyber footprint
Vendor *
2
Product *
3
Version *
4
Criticality *
Criticality Level *
5
6
Cancel
Save

1.5 Org. GDPR compliance

Procedure

Click on “My Organization” in the Main Menu

Click on “GDPR compliance” tab

Consult results of previous assessment (if any)

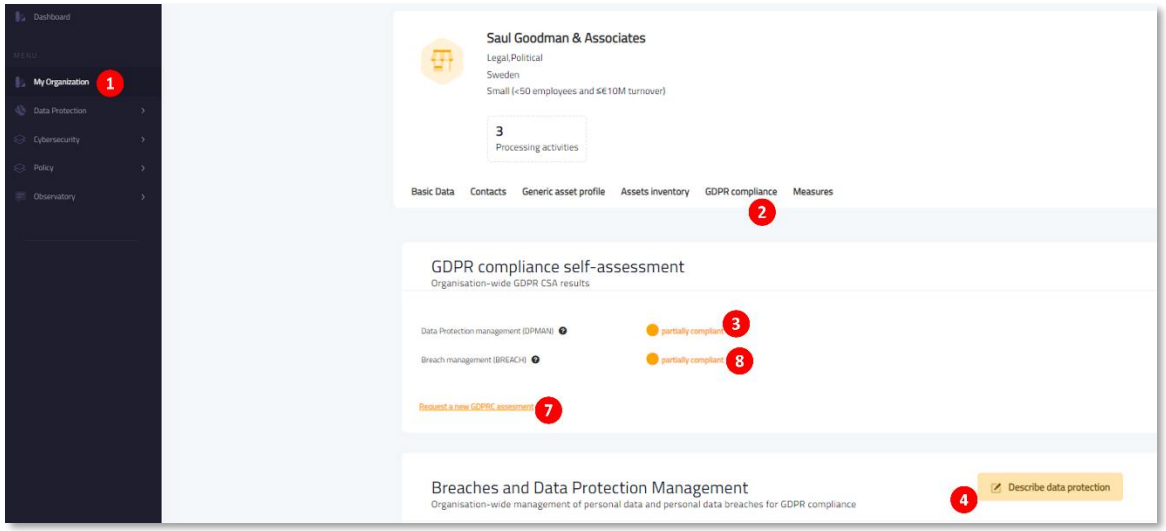
Click on “Describe data protection”

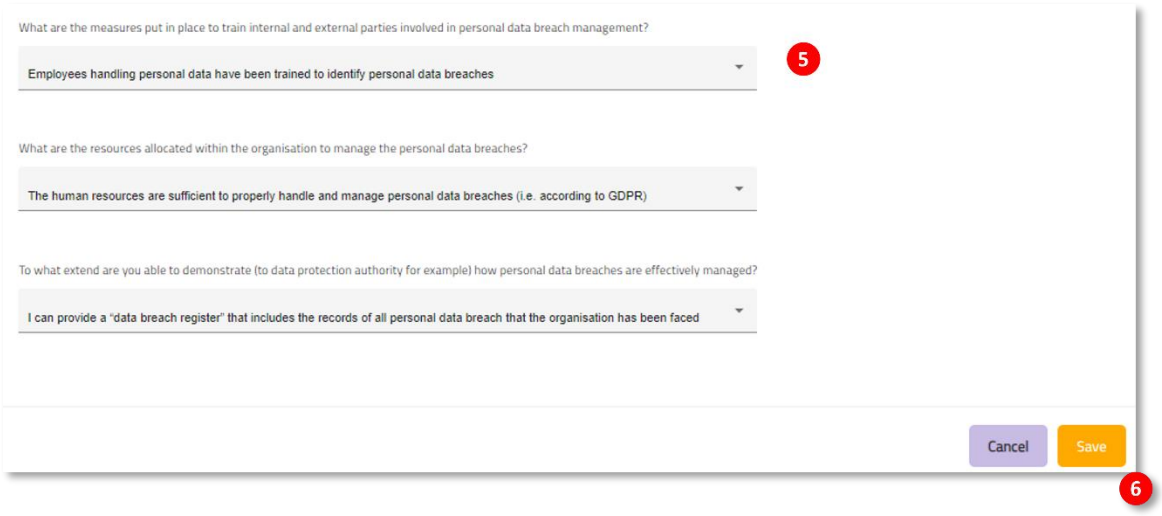
For each question, select one or more answer(s) from the corresponding drop-down list

Click on “Save”

Click on “Request a new GDPRC assesment”

Consult the compliance level of Data Protection Management and Data Breaches Management processes




What are the measures put in place to train internal and external parties involved in personal data breach management?
Employees handling personal data have been trained to identify personal data breaches
5
What are the resources allocated within the organisation to manage the personal data breaches?
The human resources are sufficient to properly handle and manage personal data breaches (i.e. according to GDPR)
To what extend are you able to demonstrate (to data protection authority for example) how personal data breaches are effectively managed?
I can provide a "data breach register" that includes the records of all personal data breach that the organisation has been faced
Cancel
Save
6

1.6 Org. Measures (OTMs)

Procedure

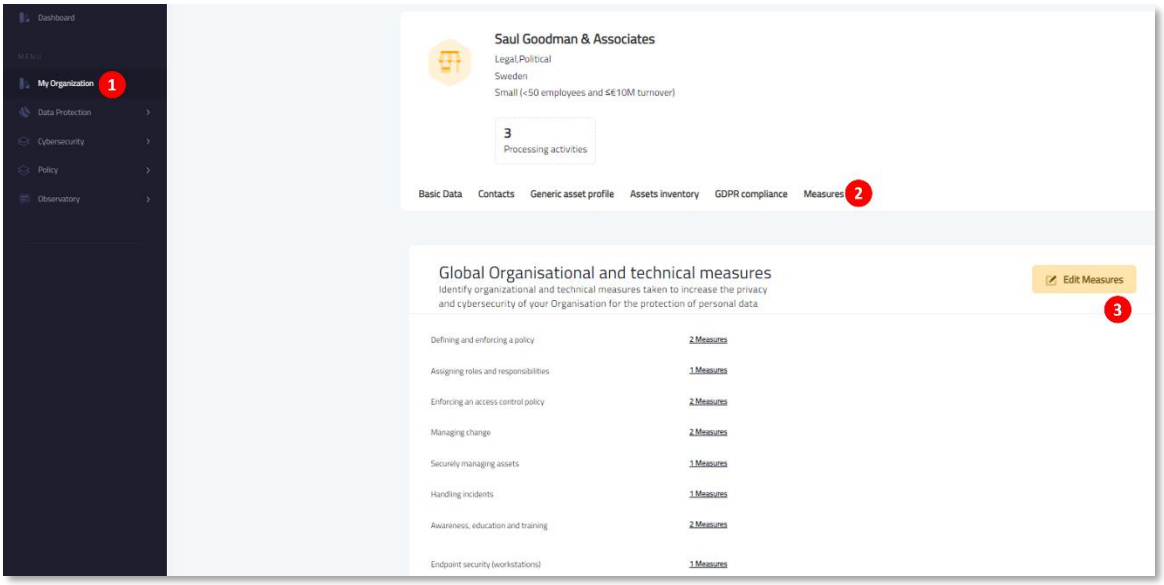
Click “My Organization on the Main Menu".

Click “Edit Measures".

Use the checkboxes alongside the OTMs to denote which OTMs you have implemented in your organisation.

Repeat the process for all of the global categories.

Click “Save”.



Create and populate one or more personal data processing activities (PAs).

Processing Activities (PAs): Information regarding the handling of personal data, represented as a provisional list of PAs and their details. The following capabilities included in creating or populating a PA:

PAs listing page (Data protection centre)

Create / edit PA page

View PA page

Create/Populate a Processing Activity (PA)

2.1 Create / edit PA page

To create a PA (e.g. Recruitment Process), from the dashboard menu select “Processing Activities” from the “Data Protection” category and edit all information needed related to the PA, including the assets operating within the process, which is organised in nine (9) information groups:

1. PA identity and basic data
2. Processing purpose
3. Data subjects
4. Data

5. Recipients

6. Risks

7. Measures

8. GDPR Compliance

9. Assets

Procedure

Click "Data Protection"/"Processing Activities" tab in the Main Menu

In the Processing Activities screen click on the Add button, or select a specific PA and click on the pencil button

In each tab, enter the information requested. You can browse through tabs clicking on Next or Previous buttons or go directly to a specific tab using the index on the left.

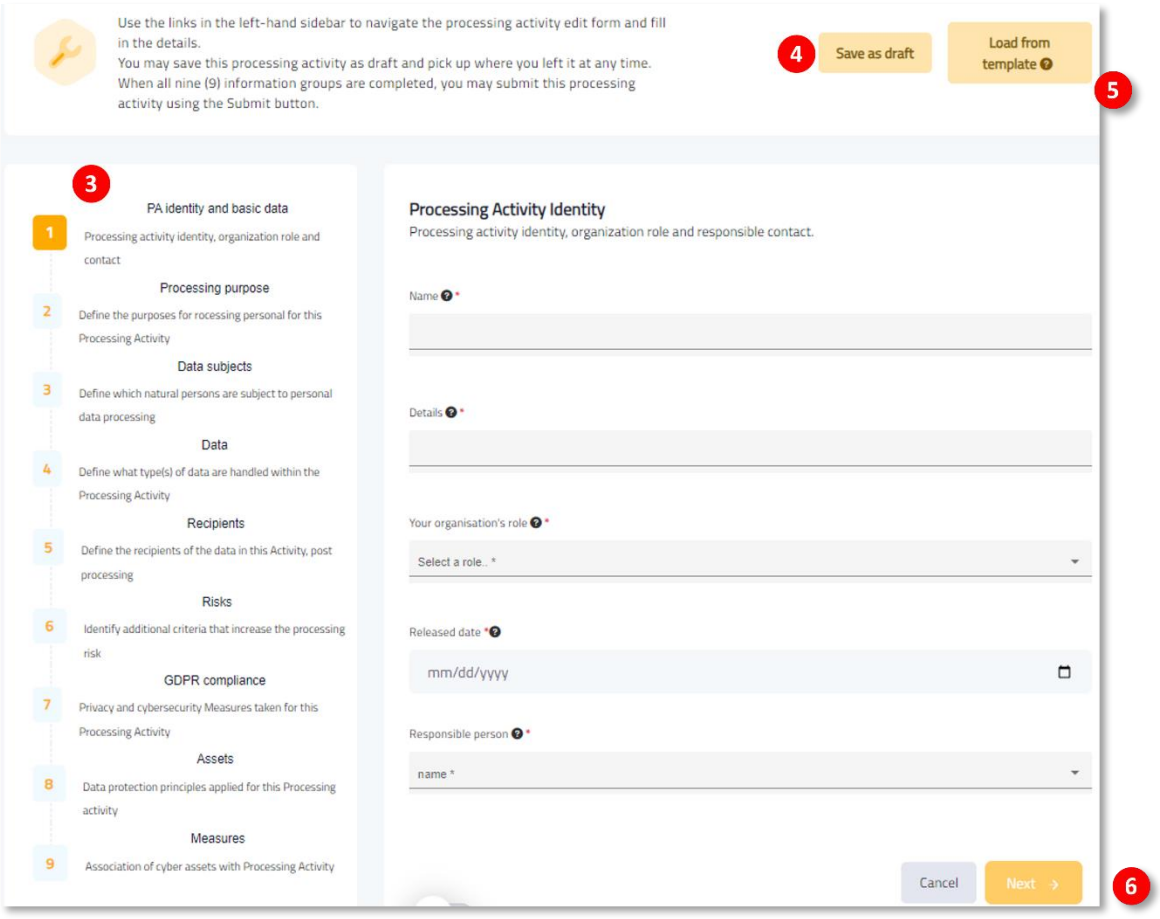
At any point you can save the PA as a draft and continue later.

By clicking on "Load from template" you can choose from a pre-filled processing activity

Once ready, you can go to Step 9 (Assets) and click Submit.

By clicking on the "pencil" icon you can edit a processing activity

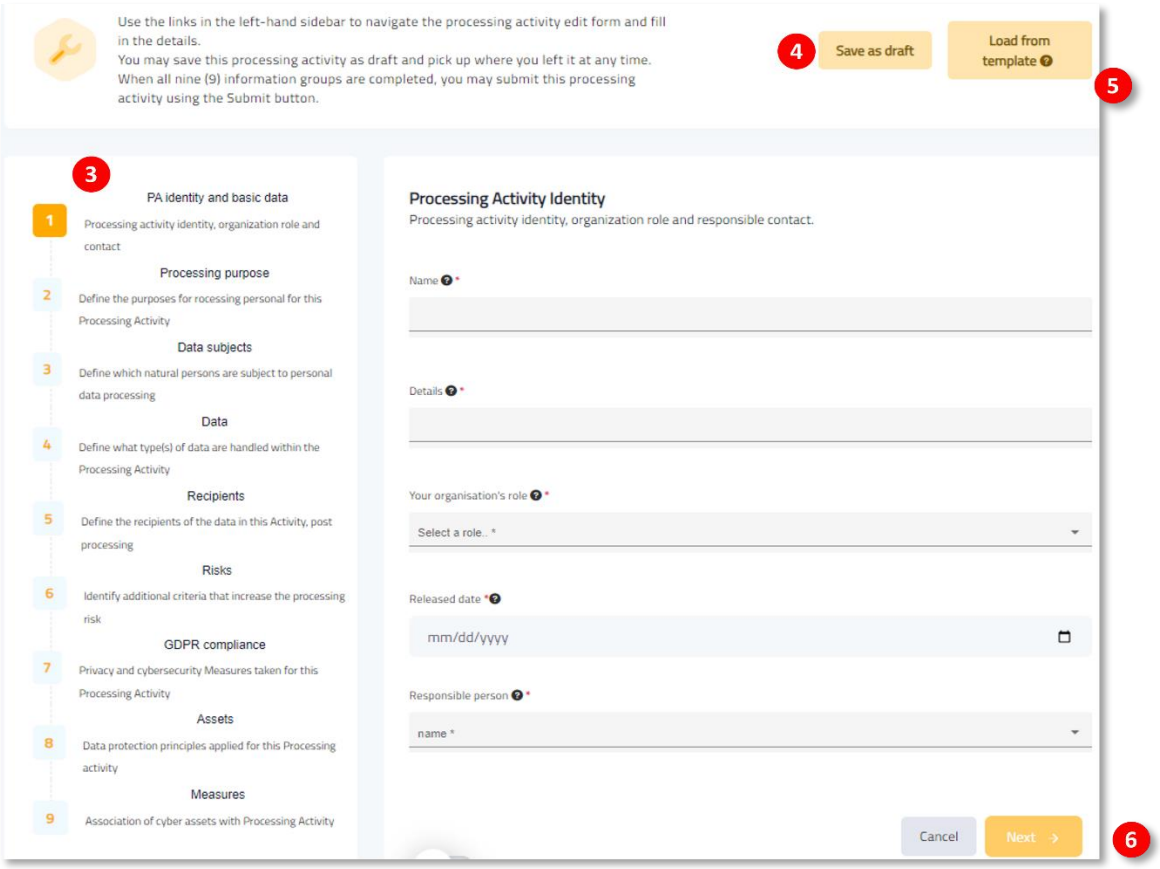
By clicking the "garbage" icon you can delete a processing activity



2.2 View PA page

Having created a processing activity, you can come back later to view or even edit that PA. For editing, repeat the same process and modify the information needed as in the creation of the PA,

In the Processing Activities screen you can view all the registered PAs In the same screen, information on the PA identity, purpose, data subjects, data, recipients, status and assessments, is provided.


Use the links in the left-hand sidebar to navigate the processing activity edit form and fill in the details.
You may save this processing activity as draft and pick up where you left it at any time.
When all nine (9) information groups are completed, you may submit this processing activity using the Submit button.
4
Save as draft
Load from template
5
3
PA identity and basic data
1
Processing activity identity, organization role and contact
Processing purpose
2
Define the purposes for rocessing personal for this Processing Activity
Data subjects
3
Define which natural persons are subject to personal data processing
Data
4
Define what type(s) of data are handled within the Processing Activity
Recipients
5
Define the recipients of the data in this Activity, post processing
Risks
6
Identify additional criteria that increase the processing risk
GDPR compliance
7
Privacy and cybersecurity Measures taken for this Processing Activity
Assets
8
Data protection principles applied for this Processing activity
Measures
9
Association of cyber assets with Processing Activity
Processing Activity Identity
Processing activity identity, organization role and responsible contact.
Name *
Details *
Your organisation's role *
Select a role.. *
Released date *
mm/dd/yyyy
Responsible person *
name *
Cancel
Next
6

Commit at least one PA to the permanent record of processing activities (ROPA)

This action, encompasses the following capabilities:

Creating a ROPA entry / committing a PA to the ROPA

Viewing a ROPA entry

Exporting a ROPA entry

Making a PA in the ROPA as inactive

Record of Processing Activities (ROPA)

The Record of Processing Activities (ROPA) is a detailed, permanent, immutable and auditable record which outlines the data processing activities carried out by an organisation. It includes information about the types of personal data processed, the purposes of the processing, the categories of data subjects involved, the recipients of the data, data transfers to third countries, and the security measures in place.

Maintaining a ROPA helps organisations demonstrate compliance with the GDPR's accountability principle (and specifically with Art. 30 of the GDPR), which requires organisations to be able to demonstrate how they comply with data protection principles. It serves as a tool for organisations to have an overview of their data processing activities and to ensure transparency and accountability in the handling of personal data.

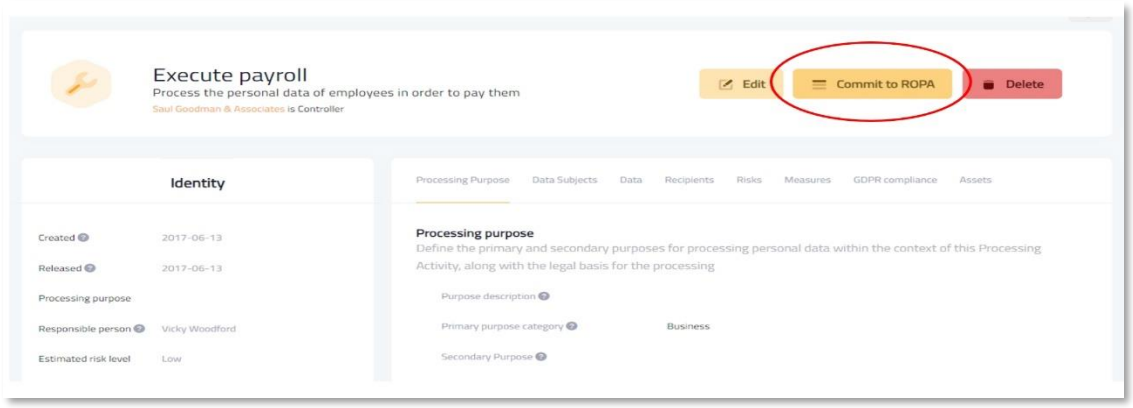
3.1 Creating a ROPA entry / committing a PA to the ROPA

Procedure

Click "Data Protection > Processing Activities" on the Main Menu and edit the PA of your choice.

When editing a regular processing activity, click on the "Commit to ROPA" button in the top of the page to permanently commit this PA to the ROPA.

Read the disclaimer text in the confirmatory dialog and click OK if you agree.



A permanent copy of the PA is now created in the ROPA.

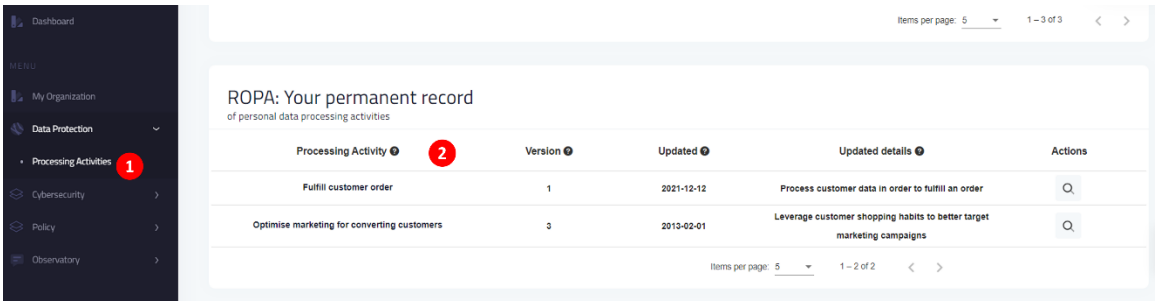
3.2 Viewing a ROPA entry

Procedure

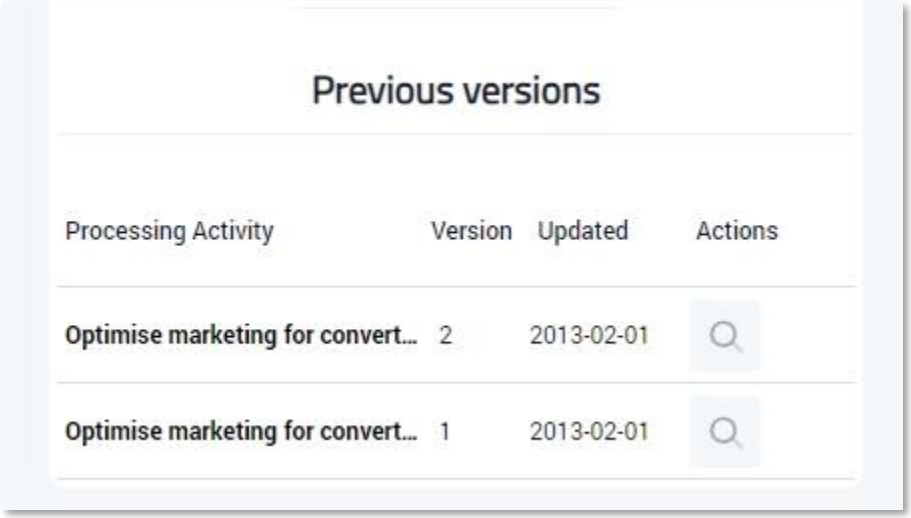
Click "Data Protection > Processing Activities" on the Main Menu

Scroll to the second part of the page called “ROPA your permanent record”, where you can see the full list of the permanent recorded processing activities.

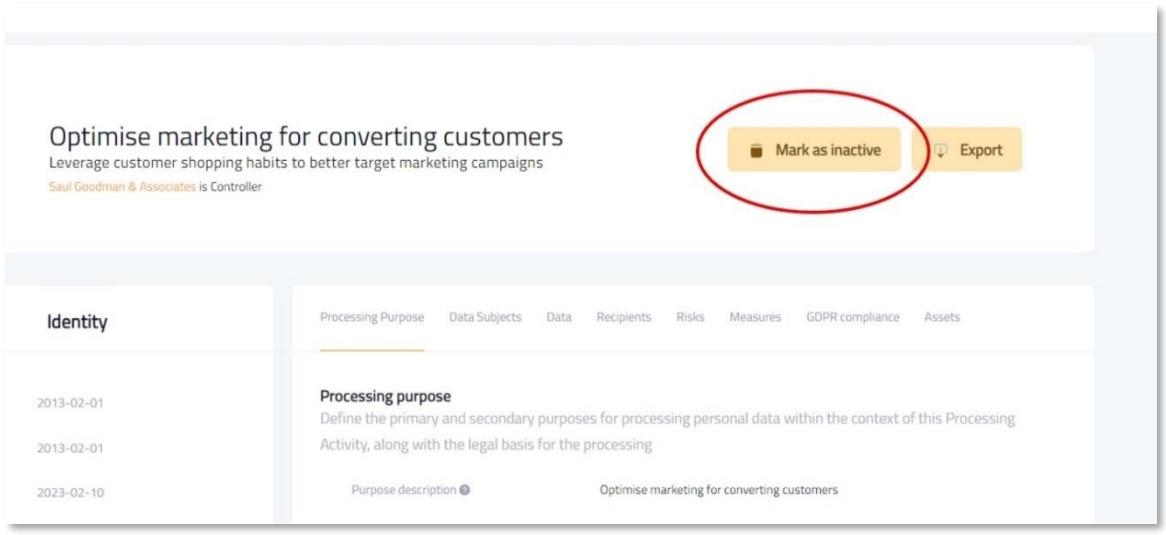
Select one to view the details.



Note that you may browse EARLIER versions of this ROPA entry if they exist, using the "Previous versions" section at the bottom of the left sidebar:

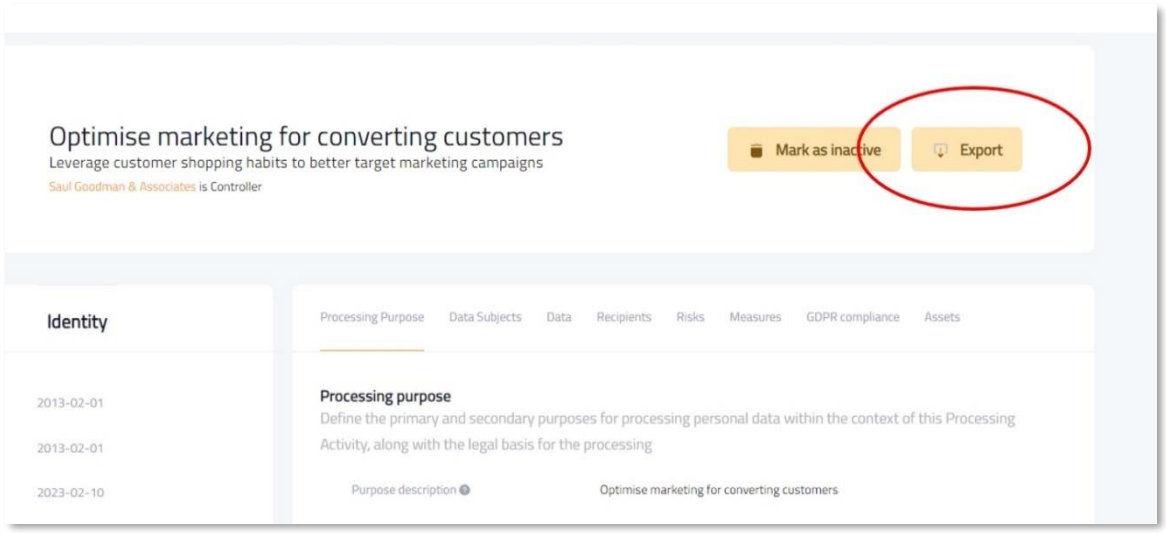


3.3 Exporting a ROPA entry



3.4 Making a PA in the ROPA as inactive

Click on the 'Mark as inactive' button to mark the CURRENT ROPA ENTRY VERSION as inactive. This functionality (currently under development) is intended for when your organisation no longer performs this specific PA in the real world, and you need to mark it as such in SENTINEL, so that an audit process might take it into account. PAs marked as inactive in the ROPA may not have newer versions saved, but older versions are still browsable, viewable and exportable.



4. Execute one or more self-assessments

The system evaluates the developed organisation profile and especially the registered PA of the experiment and decides whether the organisation is eligible for passing through the **offered assessment workflows** and implements progressively three types of assessments:

GDPR Compliance Self-Assessment.

DPIA.

Cybersecurity Risk Assessment (CSRA).

Completing an Assessment Workflow

4.1 GDPR Compliance Self-Assessment (GDPR CSA)

Definition: It determines the compliance level for the under-examination both for the specific experiment's PA.

To execute GDPR CSA on the PA for each experiment, select "Processing Activities" from the "Data Protection" category of the SENTINEL Dashboard menu and from the PAs list, choose the relevant PA and click on the "GDPRC" purple button to assess its compliance to GDPR.

4.2 Data Protection Impact Assessment (DPIA)

Definition: The DPIA is a self-assessment tool in SENTINEL, which helps determine how data processing systems, procedures or technologies affect individuals' privacy and eliminate any risks that might violate compliance for a PA. Moreover, it determines the data protection impact, likelihood and privacy risks per PA.

DPIA Purpose: The purpose of a DPIA is to assess the potential impact of a data processing activity on individuals' privacy rights and to identify measures that can be taken to mitigate or eliminate any potential risks. It's particularly important for processing activities that are likely to result in high risks to individuals' rights and freedoms, such as processing sensitive personal data or engaging in large-scale data processing.

When a DPIA is required?

A DPIA is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is required at least in the following cases:

a systematic and extensive evaluation of the personal aspects of an individual, including profiling;

processing of sensitive data on a large scale;

systematic monitoring of public areas on a large scale.

The DPIA should be conducted before the processing and should be considered as a living tool, not merely as a one-off exercise. Where there are residual risks that can't be mitigated by the measures put in place, the DPA must be consulted prior to the start of the processing.

To interpret the DPIA risk levels (High/Medium/Low), you may explore the following table:

Risk Level	Data Process Impact Assessment
High	High risk signifies that the activity or process being assessed poses a significant threat to individuals' rights and freedoms or to the organization itself. It typically implies that there is a substantial likelihood of severe harm or adverse consequences if risks are not adequately addressed. High-risk processing activities may involve sensitive personal data, large-scale data processing, or processing activities with a high potential for data breaches or misuse. Organisations should prioritise mitigating high-risk scenarios and implementing robust risk reduction measures
Medium	Medium risk suggests that the activity or process has the potential to cause harm or adverse consequences, but the likelihood or severity of these consequences is not as significant as in high-risk scenarios. Medium-risk situations may require measures to mitigate the identified risks, but these measures may not need to be as extensive or urgent as those for high-risk situations. Medium-risk processing activities may involve personal data that is not highly sensitive or situations where the potential impact on individuals is moderate.
Low	Low risk indicates that the activity or process is unlikely to result in significant harm or adverse consequences to individuals' rights and freedoms or the organisation. Low-risk scenarios may still require some risk management measures, but these are typically less extensive and urgent than for high or medium risk situations. In the context of data protection, low-risk processing activities may involve non-sensitive personal data or activities with minimal potential for harm.

Procedure for the PA-specific DPIA

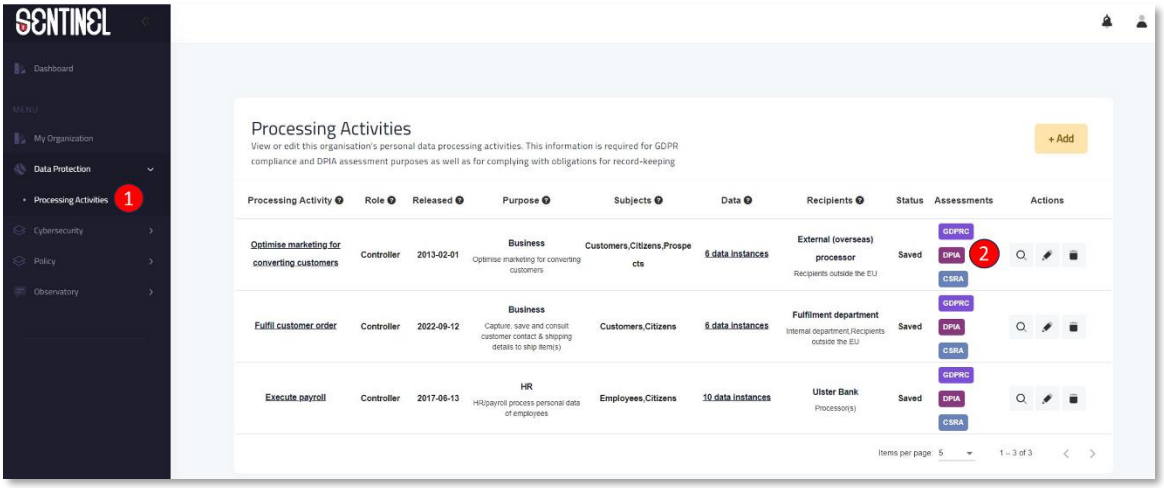
Click "Data Protection" > "Processing Activities" tab in the Main Menu

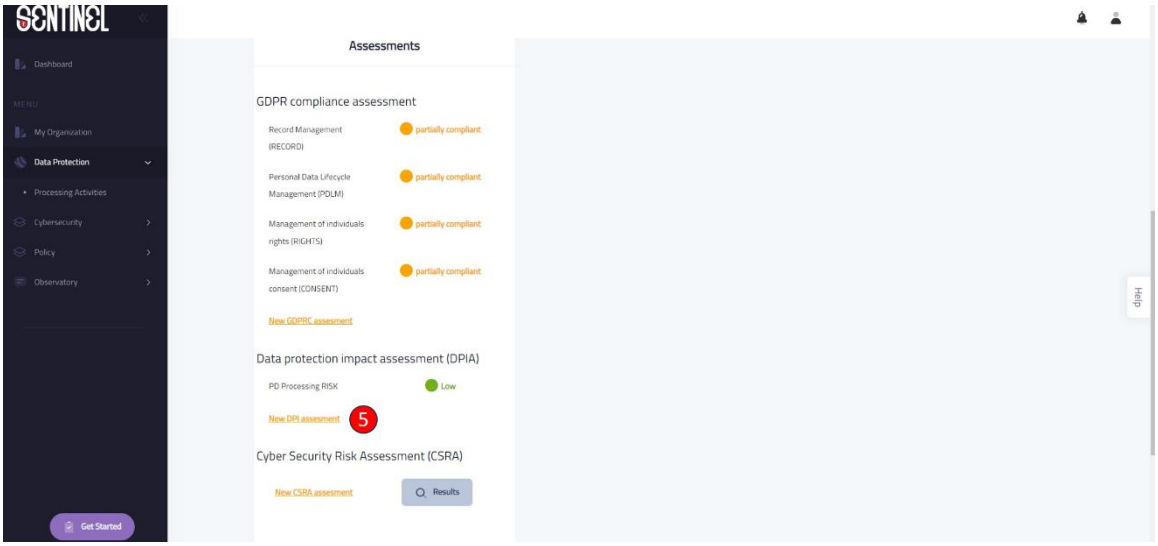
From the Processing Activity screen, click on the "DPIA" button or

Confirm your choice by clicking on the "Ok" button

Consult the results by clicking on the "Show results" button

At any time, you can consult results of previous assessments by selecting a specific PA and clicking on the "View" button. You can also request a new assessment by clicking on the "New DPIA" link below the results displayed.





Prerequisites: For a DPIA to be executed on a specific PA you are required to have provided the necessary information in the relevant step when creating or editing this PA.

Cybersecurity Risk Assessment (CSRA)

Cyber security risk management plays a critical role in managing the threats, aiming to overall system's resilience. It enables the identification of vulnerabilities and threats and the determination of suitable proactive control measures to tackle the related risks. Towards this, SENTINEL cyber security risk assessment has been identified as an essential tool for any organization, involving some of the best preventive activities to protect systems and their cyber-components. This process requires at least one cyber-asset to be successfully associated with the selected Processing Activity upon which the cyber security risk assessment will be performed.

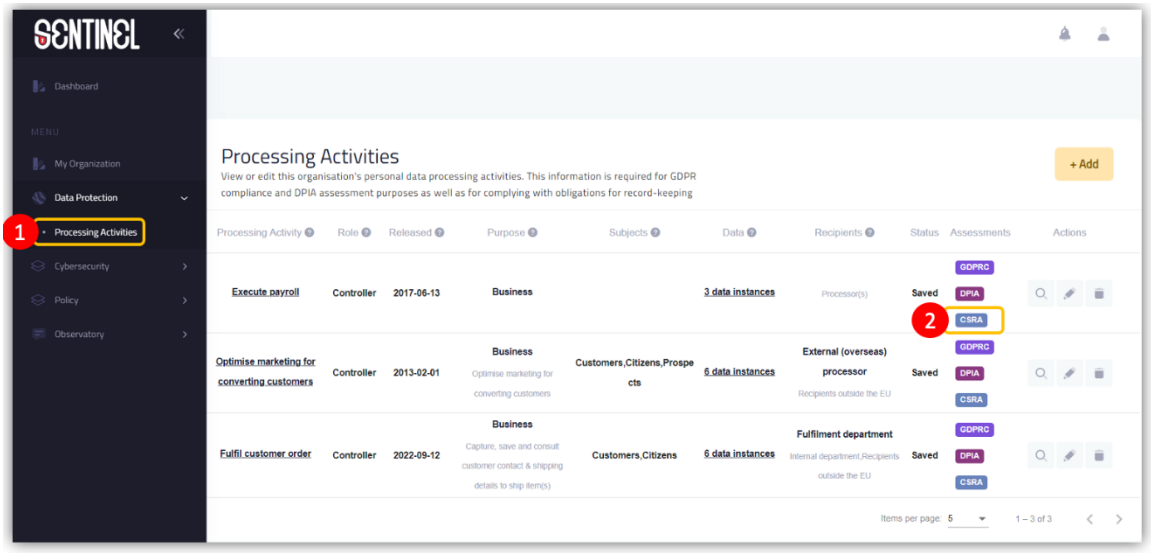
There are two different options available upon which you can initiate the process of performing a Cyber Security Risk Assessment (CSRA).

OPTION 1:

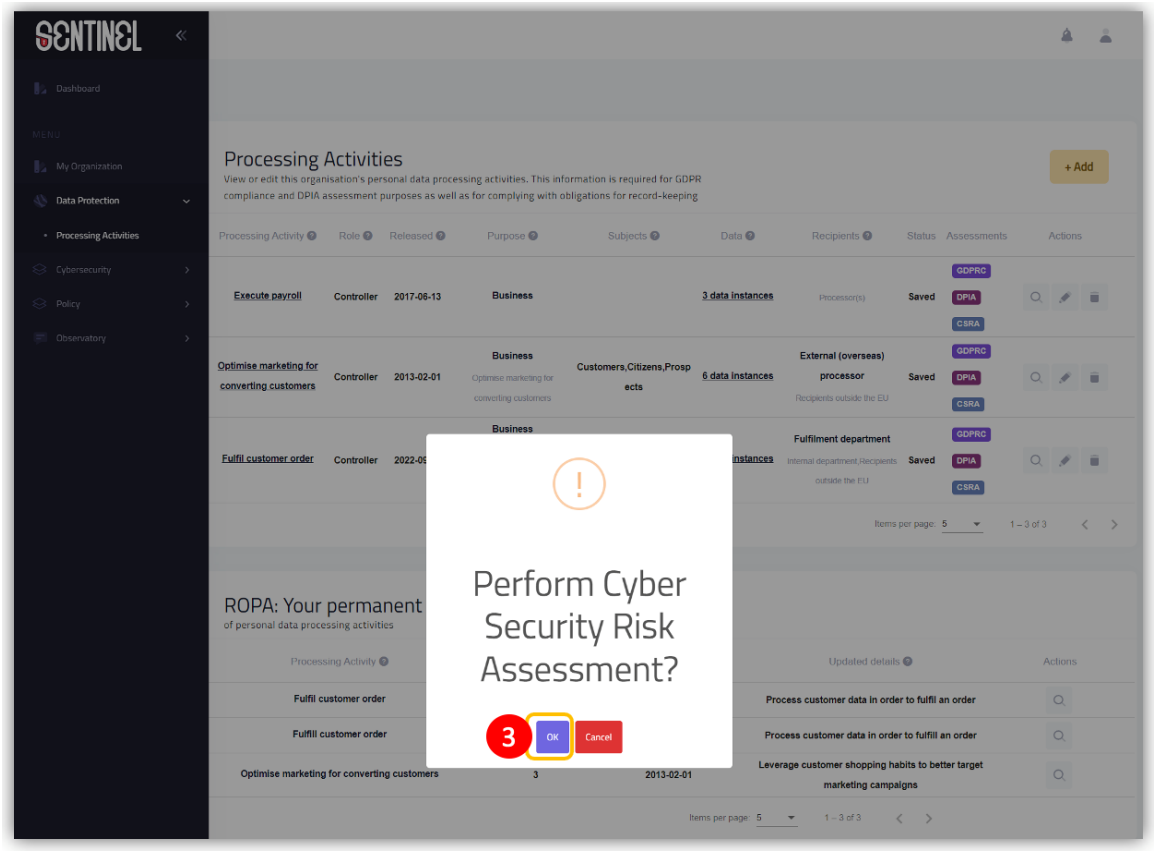
Visit SENTINEL Data Protection section

Click on "Processing Activities" on the main menu

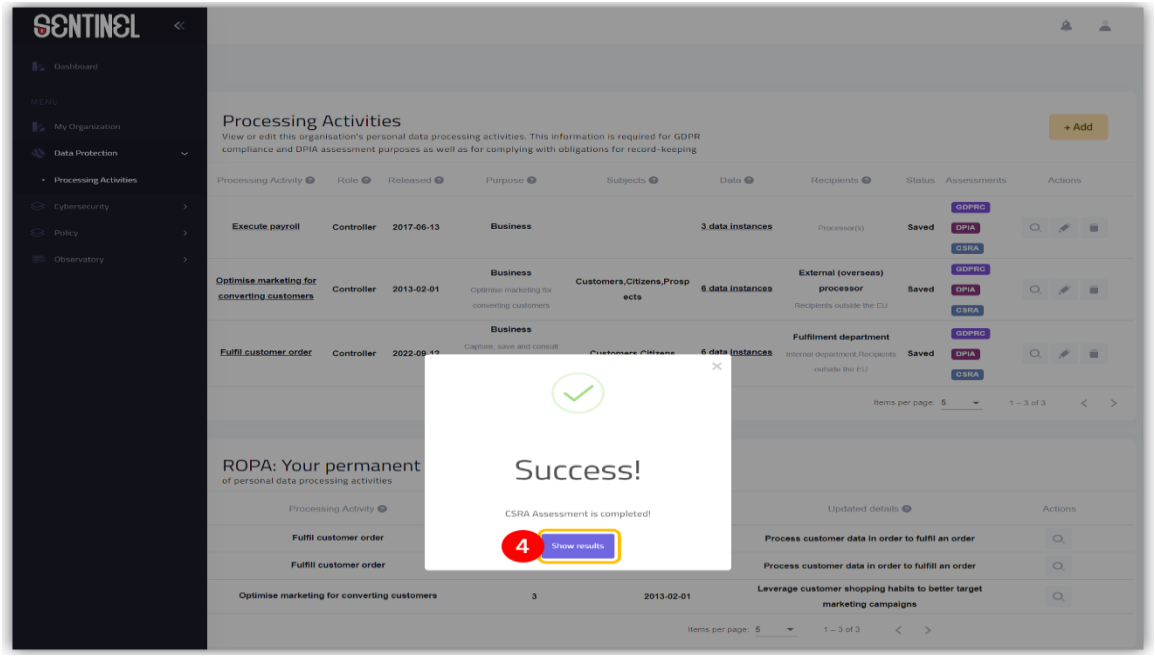
Select a Processing Activity from the list and click on "CSRA" button in order to perform a new cyber security risk assessment



Confirm your action by clicking on "Ok" button in the pop-up information window



Upon completing the calculation process a pop-up information window appears. Click on “Show results” button in order to be able to visit the analysis reports.

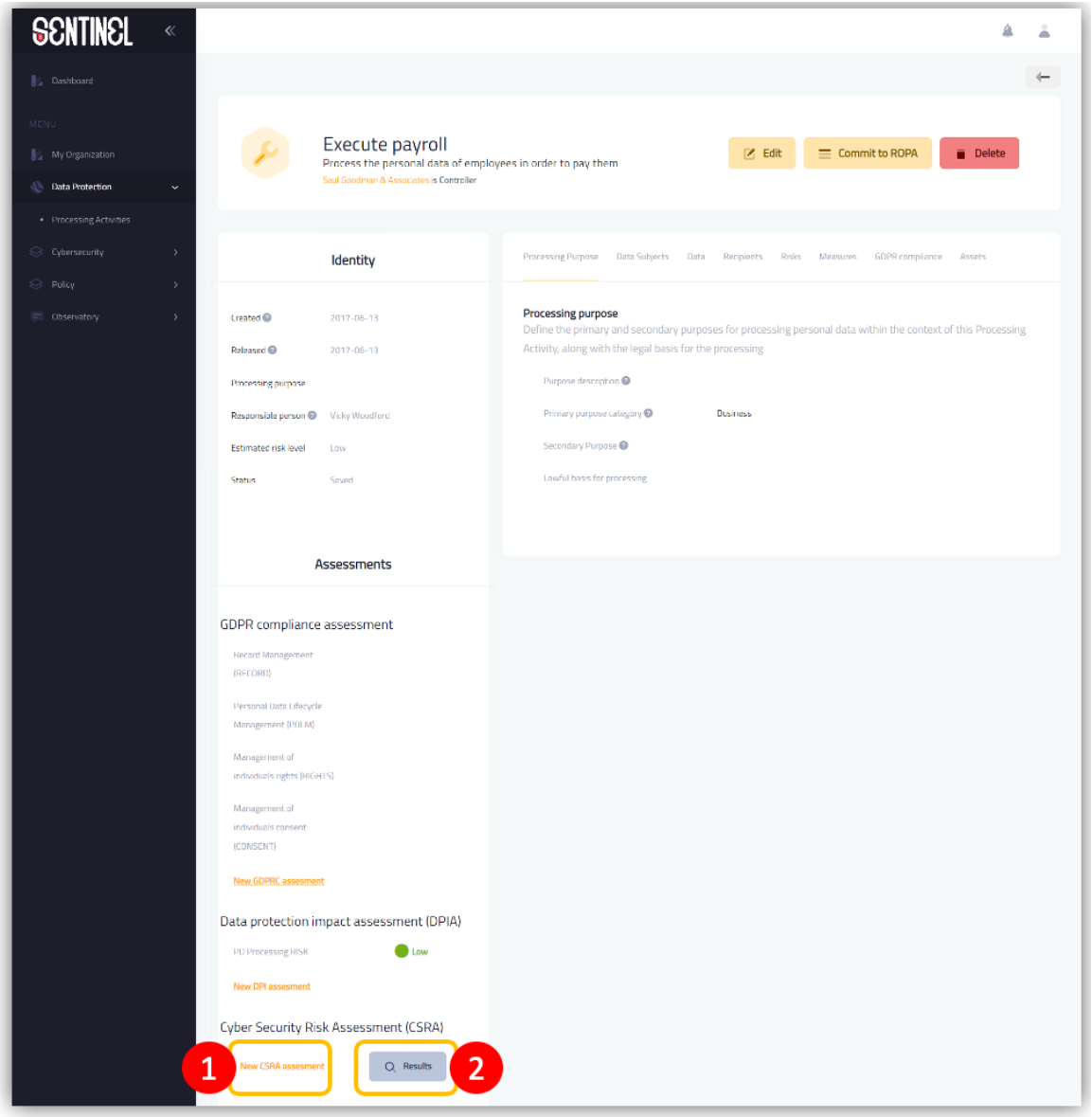


OPTION 2:

Visit the profile of your preferred Processing Activity

Click on “New CSRA” link at the Cyber Security Risk Assessment section

Alternatively, click on “Results” button to visit the analysis reports



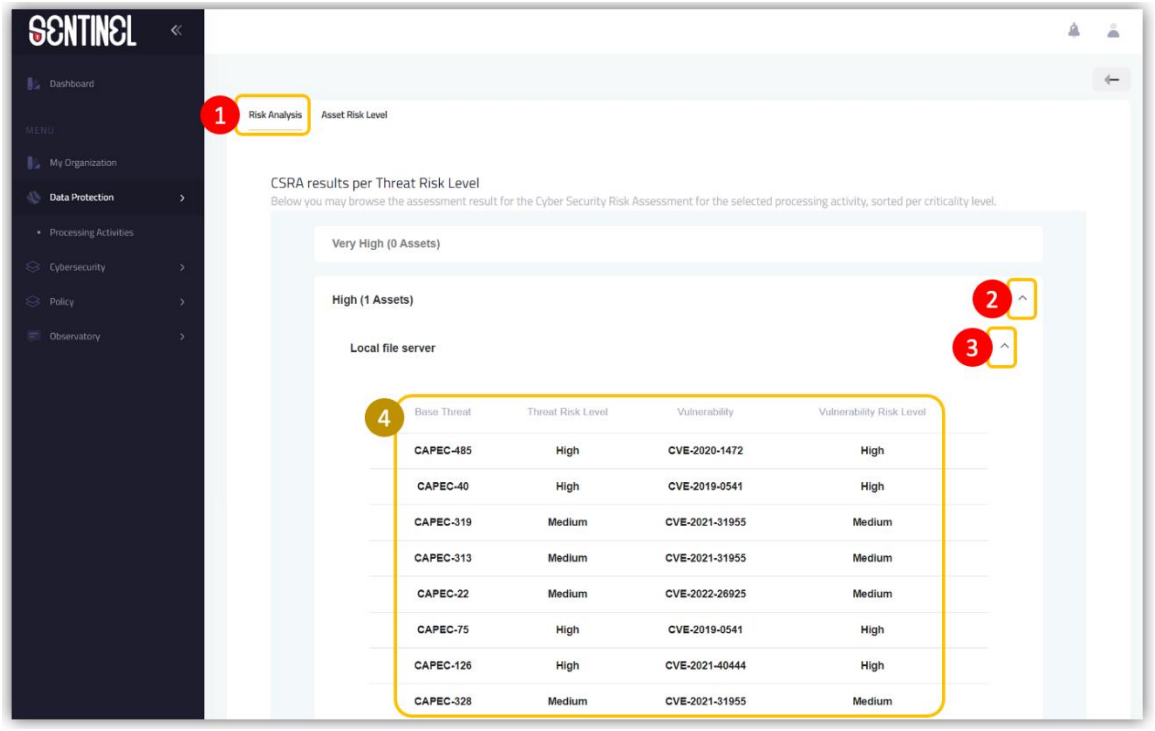
Risk Analysis report

Click on “Risk Analysis” tab in order to view the CSRA results per threat risk level

Select the risk level under which you want to view further details

Select the cyber asset which resides on this (selected) risk level

View the list of individual risks for the selected asset. Each risk consists of the threat, its risk level, the vulnerability that can be used in order to be exploited, and the impact level of the previous mentioned vulnerability



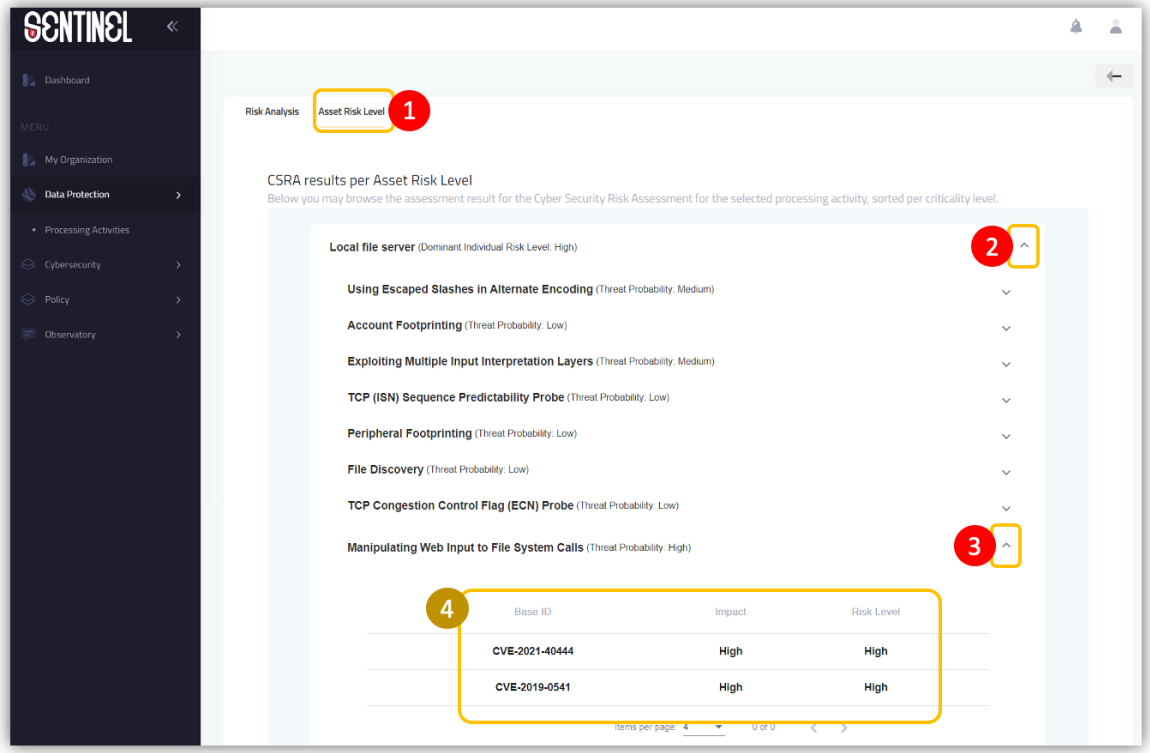
Asset Risk Level report

Click on “Asset Risk Level” tab in order to view the CSRA results per asset risk level

Select your preferred cyber asset

Select the specific threat (from a list of identified threats for this cyber asset) for which you want to view further details

View the list of vulnerabilities that can be used for the realization of the selected threat, along with their impact and the risk level

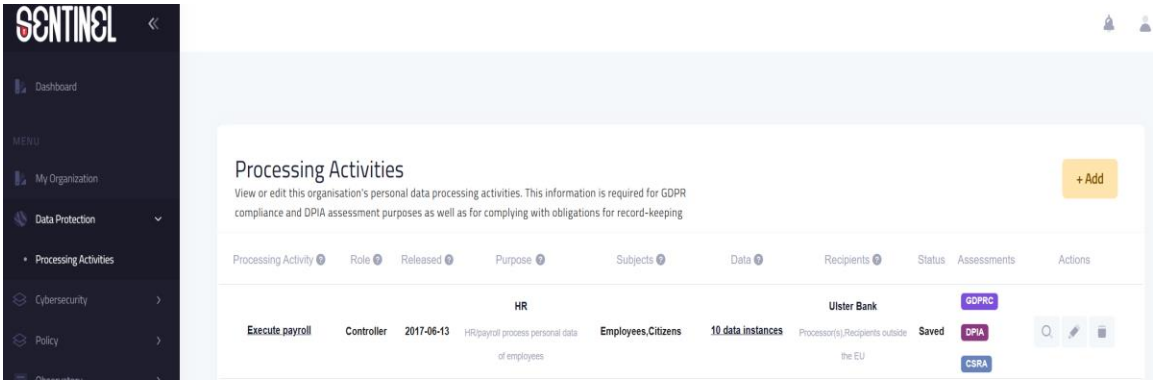


Prerequisites:

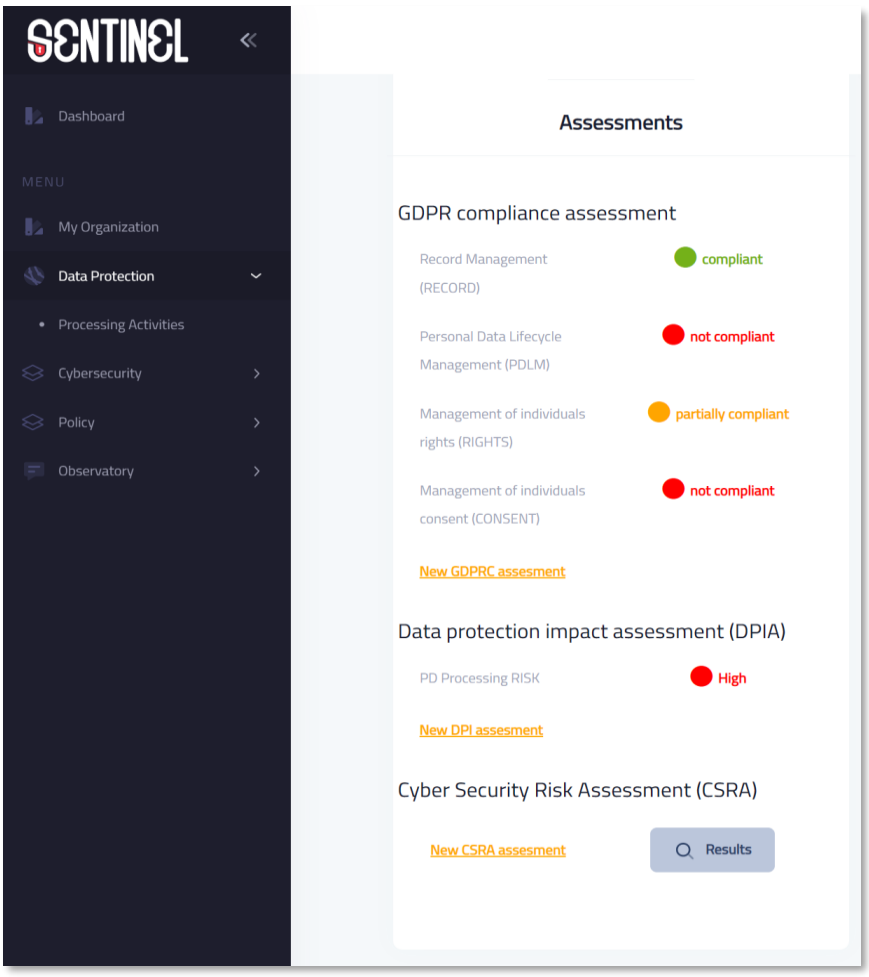
Create at least one cyber asset in the “Assets Inventory”

Associate at least one cyber asset with the Processing Activity under which the CSRA will be performed

To perform CSRA on the assets of each of the PAs (*i.e. “Dimensions Care Children Package” PA for Experiment 1, and “Safe recruitment and criminal record checks” PA for Experiment 2*), select “Processing Activities” from the “Data Protection” category of the SENTINEL Dashboard menu and from the PAs list, choose the corresponding PA and click on the “CSRA” light blue button.



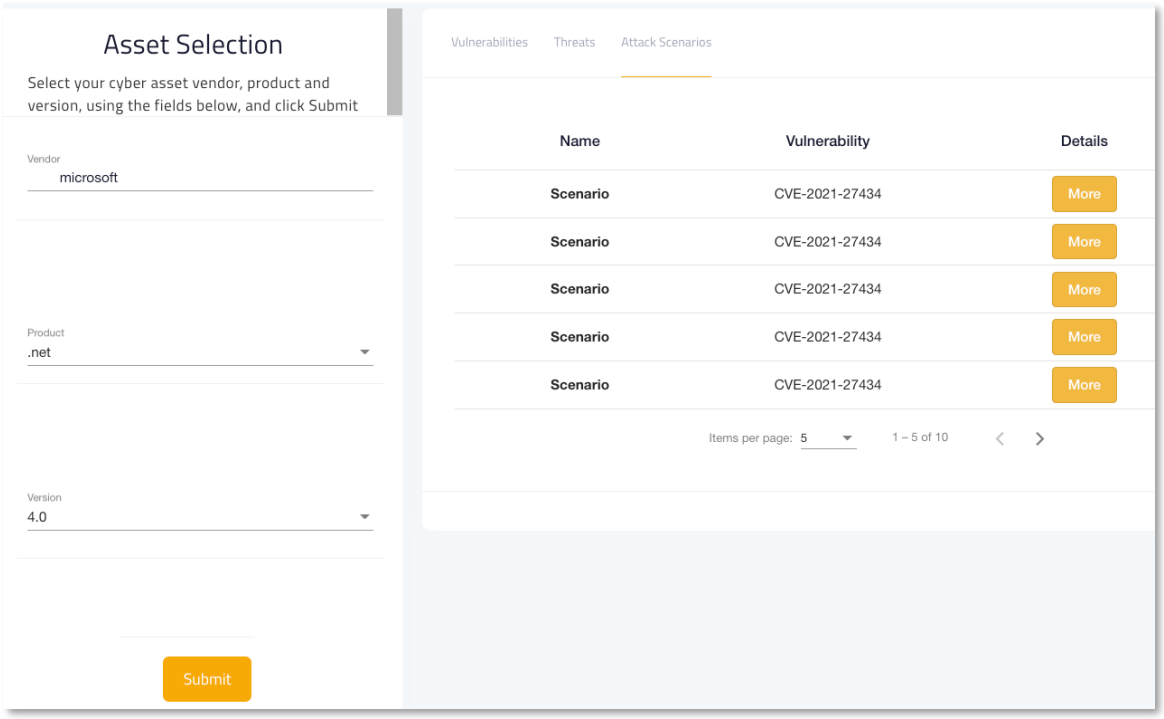
The three assessments results of each PA may be viewed by clicking upon the specific PA.



The CSRA results can be viewed by clicking on the “Results” button depicted in the previous screen: i) per threat/vulnerability levels for each asset, ii) per asset risk level.

In addition, the SENTINEL platform offers a simulation environment where the SENTINEL user may experiment on alternative attack scenarios towards the organisation's registered assets to identify corresponding security vulnerabilities and threats. This functionality facilitates IT and cybersecurity professionals either to better comprehend the produced CSRA results for a selected PA or enhance their security knowledge on organisational assets. In the current experiment, you may use the simulation environment to identify security information of the assets operating in the under-examination PA by inserting their technical characteristics and explore all potential attack scenarios (combinations of vulnerabilities and threats of the asset), as shown below. To experiment on such alternative attack scenarios upon preferred assets, the SENTINEL user may select the "Cybersecurity" category from the SENTINEL dashboard menu and click on the "Simulation Environment" option.

An indicative list of known attack scenarios for a selected asset in the Simulation Environment is displayed in the following Figure.



SENTINEL leverages data gathered during the previous steps, to calculate recommendations of measures, software and training material, tailored to your organisation.

These may be browsed under "Policy". The main purpose of Policy Recommendations is to analyse your organization profile as well as the information registered for each completed Processing Activity (PA), and propose human-readable, enforceable and actionable policy. Considering the full list of proposed recommendations, this section drafts tailor-made optimization policies for your organization regarding its technologies, tools and procedures. The proposed recommendations are grouped in two different groups:

Global recommendations

These recommendations concern the whole organization regardless of the information provided in each PA, categorized in the following topics

Defining and enforcing a policy

Assigning roles and responsibilities

Enforcing an access control policy

Securely managing assets

Managing change

Handling incidents

Cybersecurity awareness, education and training

Endpoint security – workstations

Endpoint security – mobile devices

Physical security

PA-specific recommendations

The recommendations are related to individual PAs, categorized in the following topics:

Managing data processors for the GDPR

Managing human resources

Authentication and access control

Logging and monitoring

Server and database security

Network security

Backup policy

Application lifecycle security

Data disposal

Each recommendation comes with a brief description and its implementation status along with a list of proposed software tools and a list of relative and available training material.

Acquiring Policy Recommendations

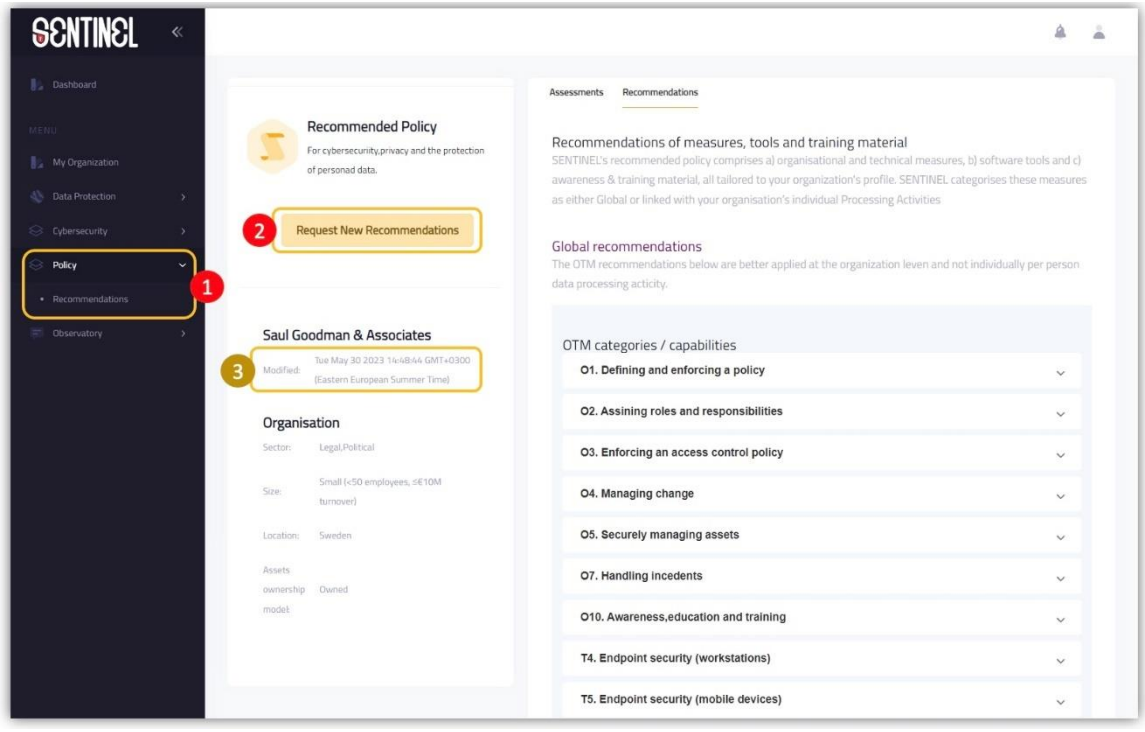
Procedure

Visit SENTINEL Policy Recommendations section

Click on “Policy” / “Recommendations” on the main menu

Click on “Request New Recommendations” button in order to generate a new SENTINEL Policy consisting of proposed recommendations.

Upon generating a SENTINEL Policy, this will be available till the next time you will generate a new one. The date and time of creation of the latest generated Policy is always visible and available on your screen.



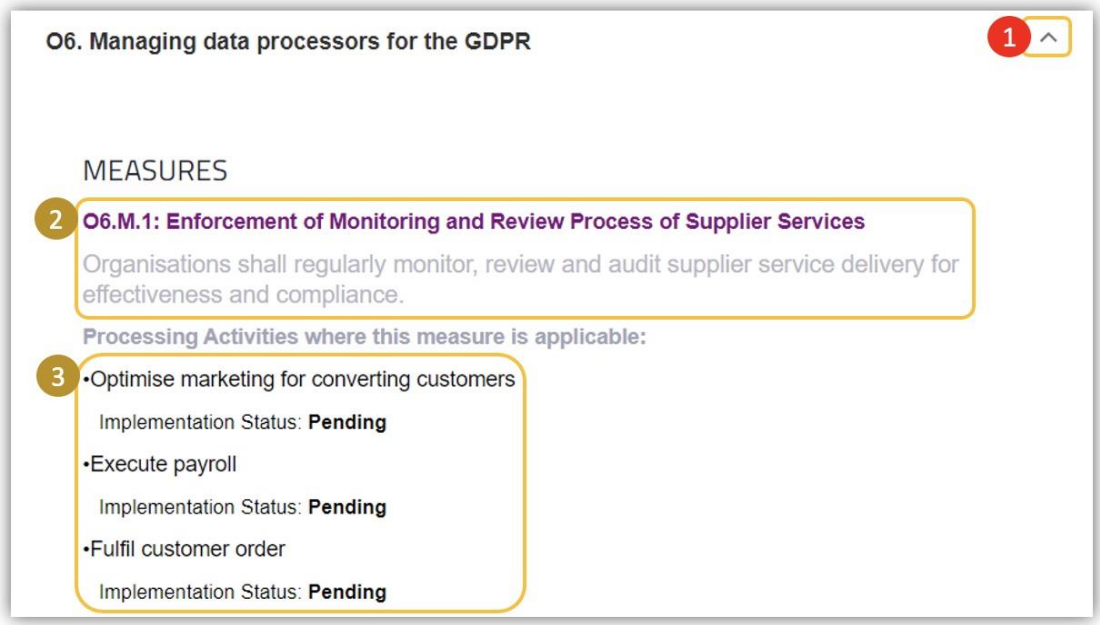
Review your organization’s assessment results, selecting the tab entitled as “Assessments” MISSING

Review SENTINEL recommendations

Select the tab “Recommendations” in order to visit your organization’s recommended security and privacy measures. These are grouped in two different categories “Global recommendation” and “Recommendations related to individual PD processing activities”

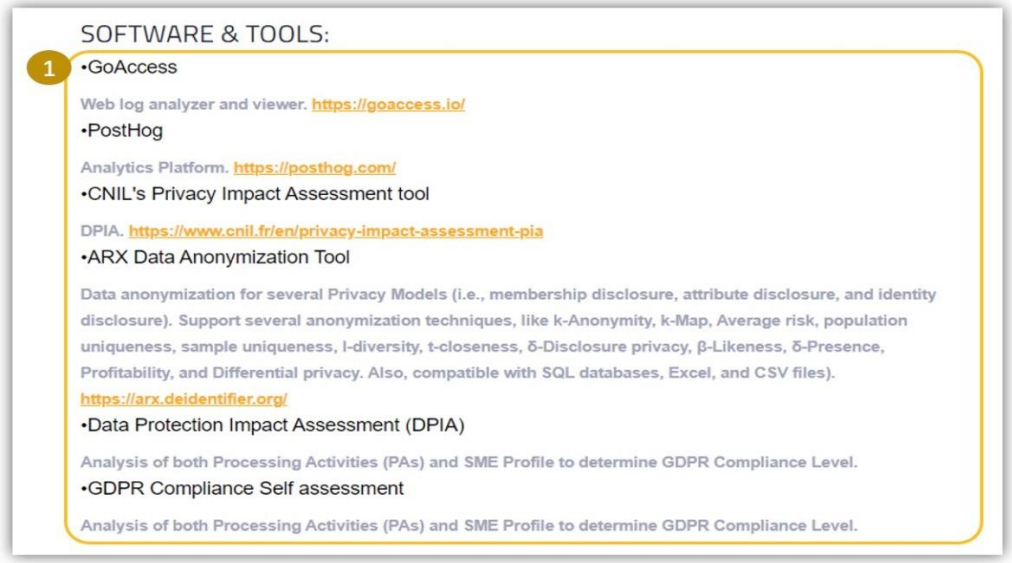
Select a recommendation in order to get informed of its details (i.e. description, implementation status, proposed software tools, available training materials)

Get informed of the proposed recommendation from its description, and review its implementation status in your organisation



Review list of recommended Software & Tools

Check the list of proposed software and tools that you may use in order to successfully address the recommendation or cover specific aspects of it



Review list of available Training Materials

Check the list of the available training materials that will help you to better understand, decide on actions to be taken, and/or address the proposed recommendation within your organisation

Prerequisites:

(Required) Create Organization Profile (hyperlink) in order to get global recommendations

(Optional) Create new PA (link) for getting recommendations related to individual PD processing activities

(Optional) Perform a GDPR assessment in order to view its results

(Optional) Perform a DPIA-assessment in order to view its results

(Optional) Perform a CSRA assessment in order to view its results

SENTINEL keeps track of which recommended measures are implemented by each organisations, and which measures are still pending.

After receiving a set of tailor-made security and privacy policies, the SENTINEL user may track the “implementation status” of the OTMs related to each pilot experiment contained in the policy draft.

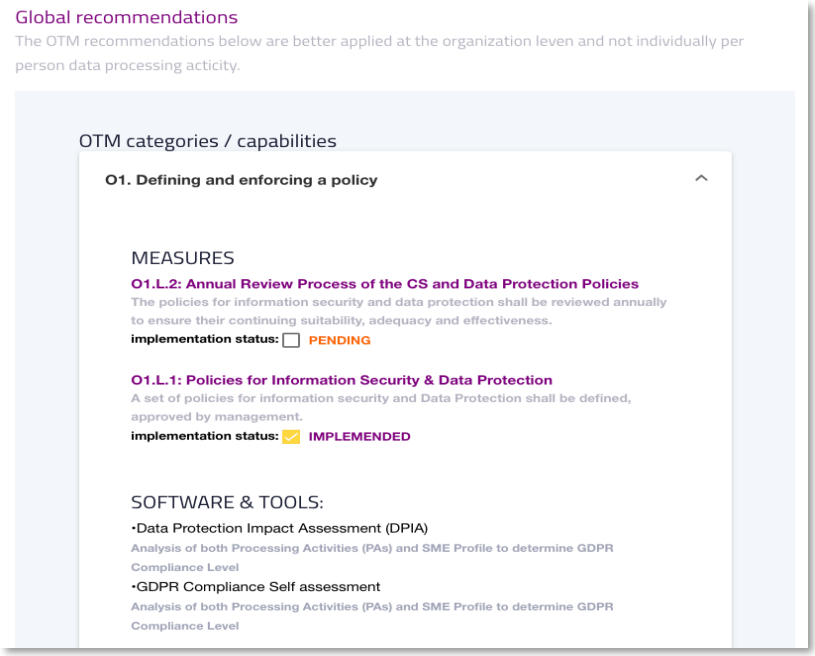
Policy Monitoring

The “implementation status” may result in one of the following:

Not implemented (for OTMs which are neither recommended nor implemented)

Pending (for OTMs which are recommended but not implemented)

Implemented (for OTMs which are implemented regardless of whether they are recommended or not)



Explore the CyberRange interface

Explore the CyberRange interface to recreate the cyber setup of your organisation and learn how to do cyber defense. Play around in the new CyberRange gaming interface to discover best cyber defense practices in action.

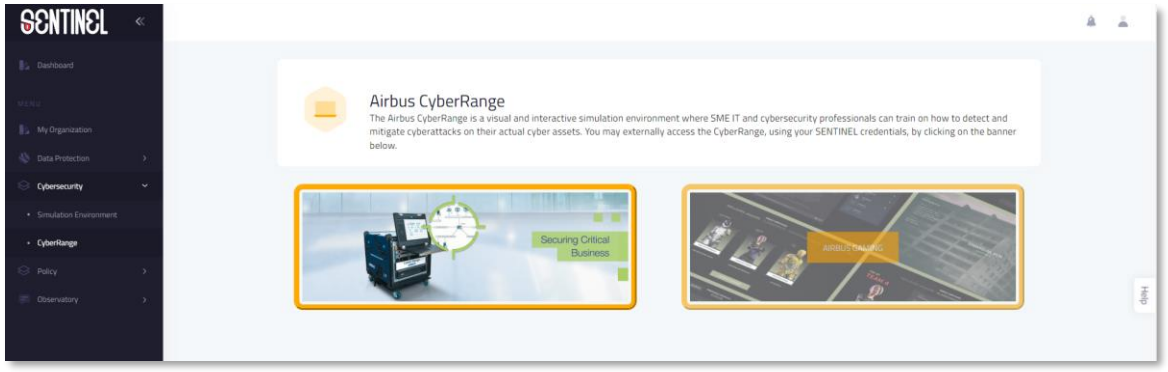
The Airbus CyberRange gaming interface is an external simulation service for hands-on cybersecurity training which aims to raise the user's awareness. In this regard, users will learn in an interactive way the best practice to better protect personal and sensitive data.

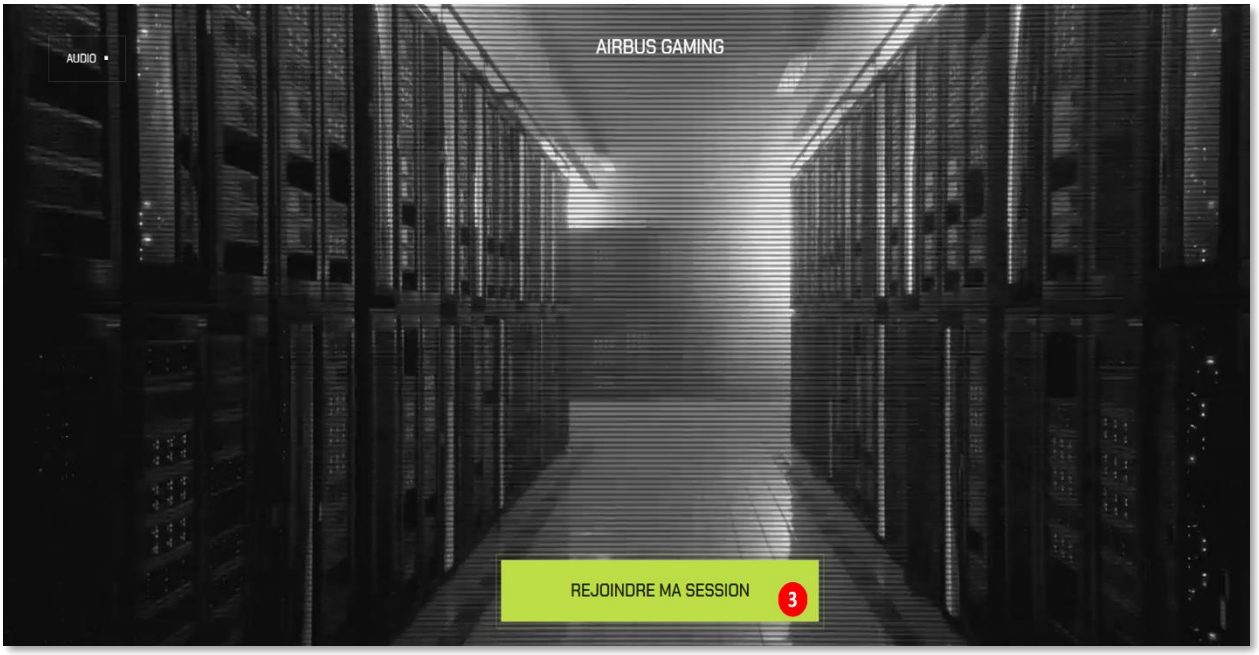
CyberRange Gaming

Procedure

Click "Cybersecurity>CyberRange" tab in the Main Menu

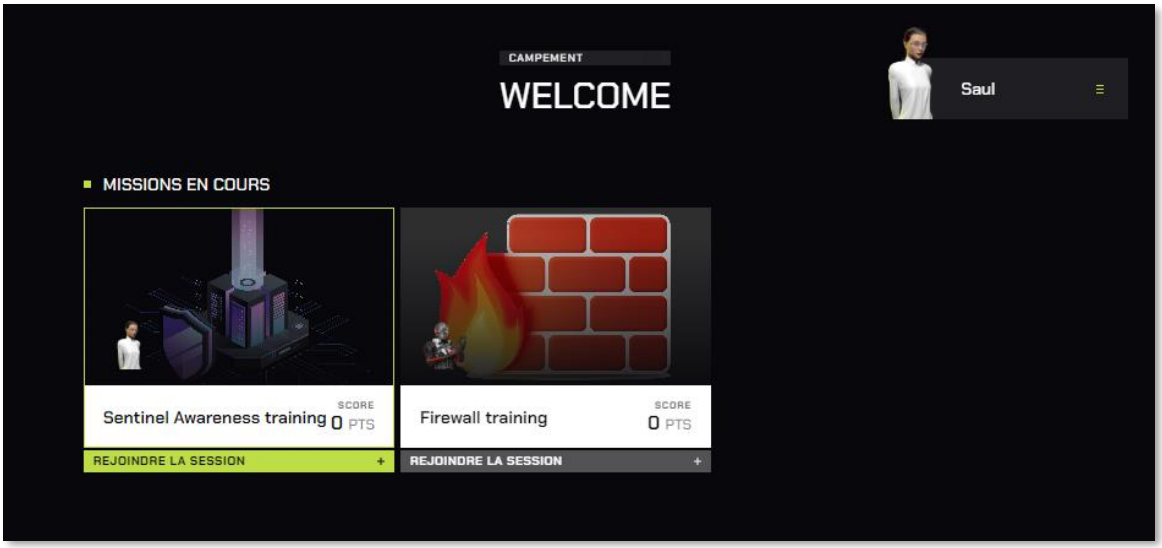
Sign in to the CyberRange Airbus gaming interface (From Sentinel Platform or on https://gaming-heracles.cyberrange.cloud/)



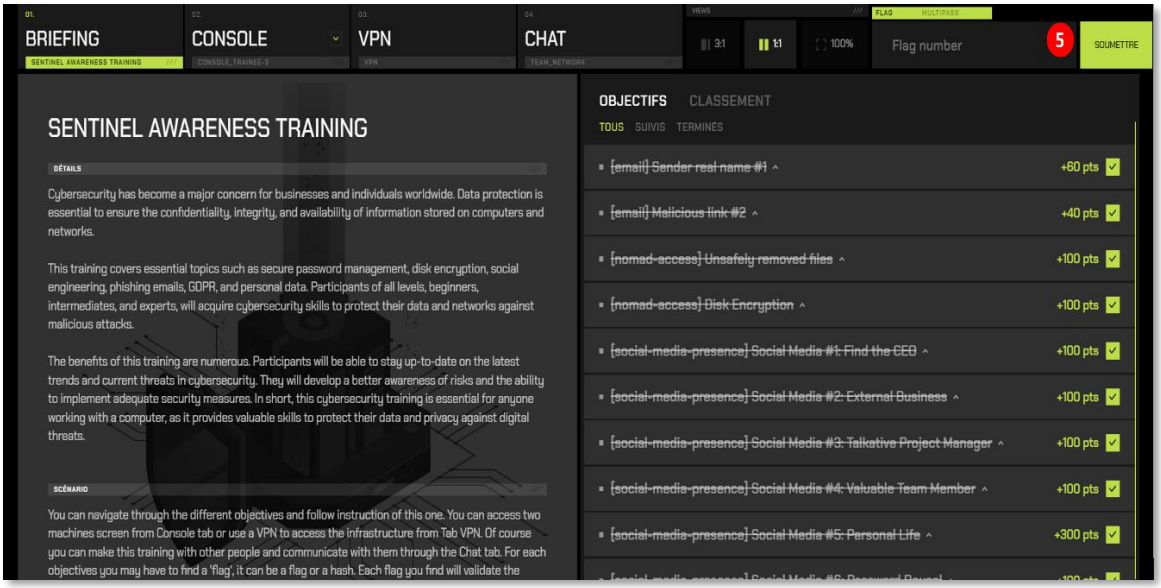


Join the session

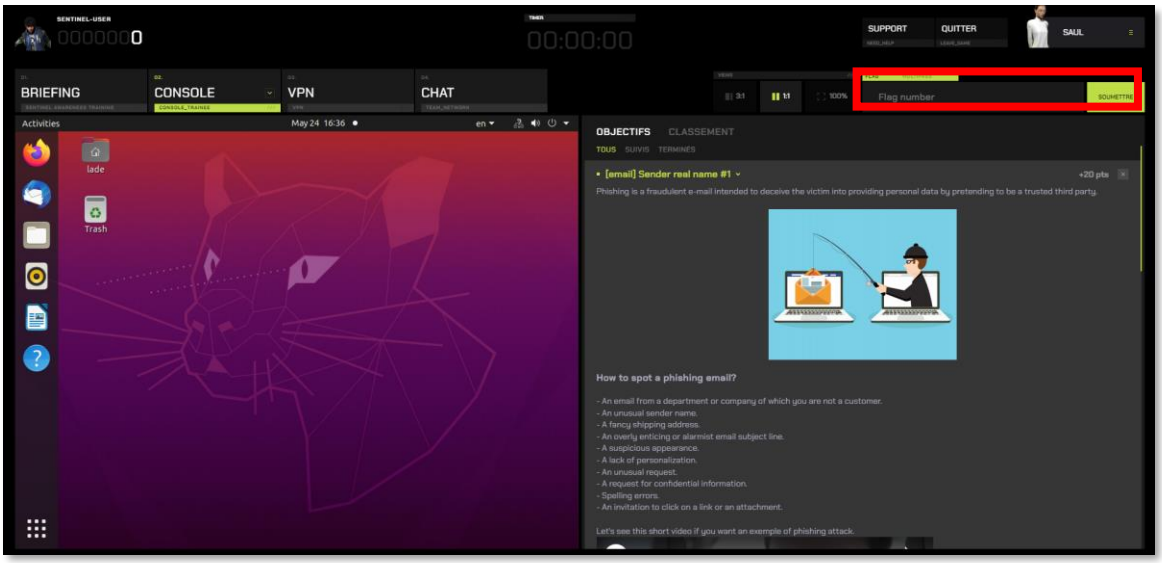
Choose your mission: “Sentinel Awareness training”



Perform the training: After reading the briefing, you can click on the objectives to view the instructions. Follow the instructions of the objective to perform the training.



To validate an objective, write the Flag in the “Flag number” textbox and click on “SUBMIT”



Depending on the objectives, a different console can be needed, you can choose the one you want to access from the list.


SENTINEL-USER
0000000
01.
BRIEFING
SENTINEL AWARENESS TRAINING
02.
CONSOLE
CONSOLE_TRAINEE
03.
VPN
_LIST
TRAINEE
WIN10
04.
CHAT
TEAM_NETWORK

Explore the Observatory

The user may browse the Observatory to explore:

Up-to-date information on the latest threats and vulnerabilities data from open threat intelligence platforms (for expert and technical cybersecurity staff)

Handling incidents and reporting/sharing them to the appropriate communities.

Selected and curated content and training material on best practices for cybersecurity and data protection.

The user may browse the Observatory either from the “Threat Intelligence” page or from the “Knowledge Base” page as described in the following.

Browsing the Observatory

8.1 Observatory | Threat Intelligence

The Threat Intelligence page of the SENTINEL Observatory provides access and monitoring of a number of open security data sharing platforms with the added capability of sharing incident or breaches and propagating the data to the appropriate third-parties or communities.

Users can consult this page and access information about recently identified data and privacy breaches.

Users can also report an incident that they faced and contribute back to the community.

This page is supported by two different instances of the Malware Information Sharing Platform (MISP), which is an open-source threat intelligence platform.

By browsing the list of provided threats, the user can select or directly search for a specific topic that they believe might affect their organization.
Each table entry is an incident which refers to a specific event that involves security-related incidents, such as a cyberattack, data breach, or any other noteworthy security event. Each of the incidents can contain multiple attributes, which refer to a specific piece of information associated with an event or an indicator of compromise (IOC).

Procedure

Click "Threat intelligence" in the Main Menu

The landing page of this topic opens in the Sentinel MISP Instance incidents.

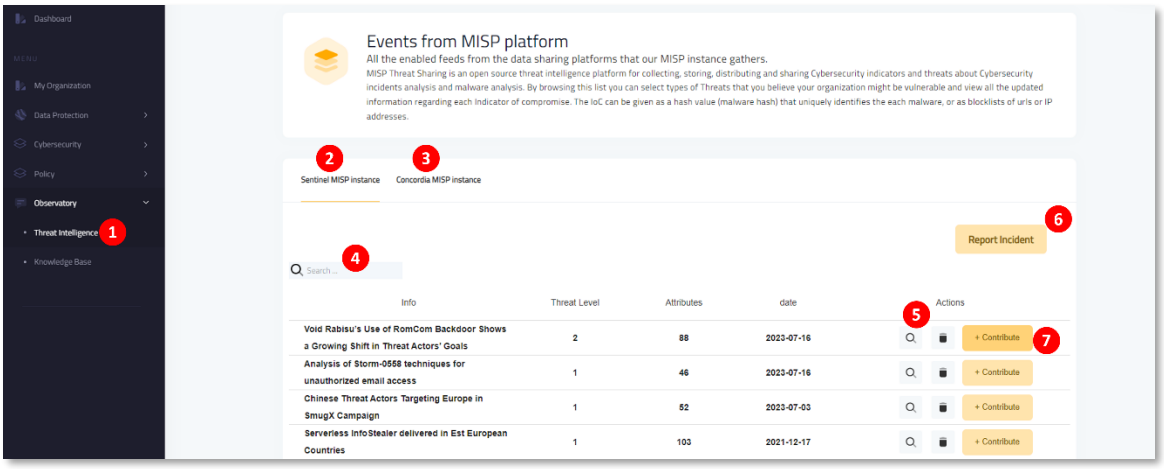
You can also view the MISP instance of another EU-funded project: www.concordia-h4020.eu

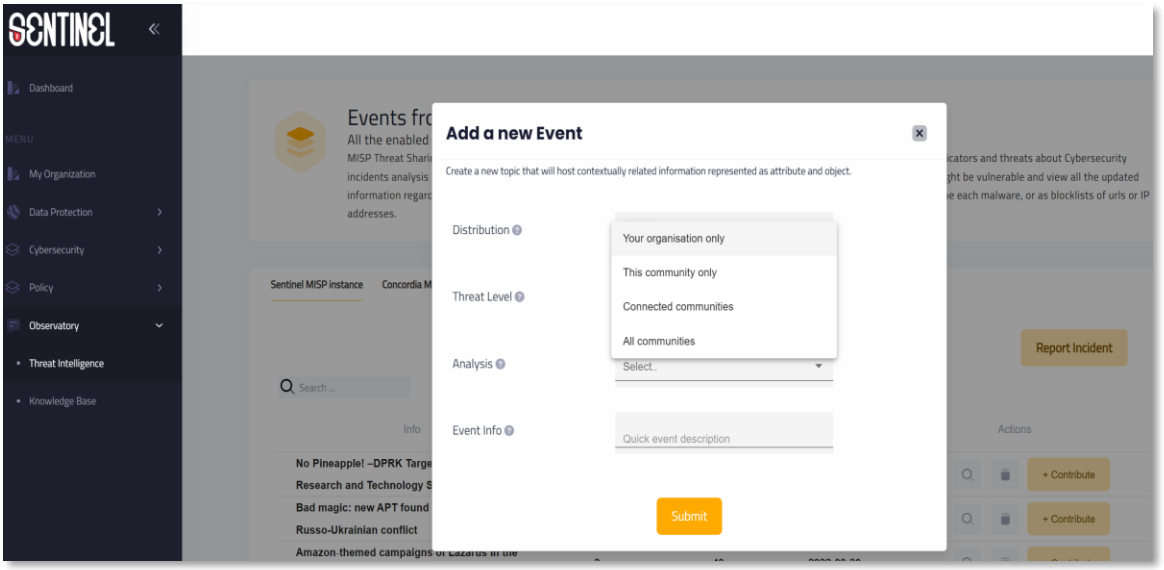
You can search for a specific topic or IoC from the Search filter

When an interesting topic has been found, you can open it and investigate its relevant attributes.

You can report a new incident that you might have faced.

You can contribute to an existing incident by adding a new attribute. (The exact theat info/data that you faced)





Prerequisites: A technical background greatly facilitates the comprehension and interpretation of this page.

8.2 Observatory | Knowledge Base

An interface to open vulnerability and threat repositories. The Knowledge Base contains a list of threats and vulnerabilities detected by known libraries. For each detected vulnerability a short description is provided alongside the products affected, weaknesses and related threats, similarly for the threat repository, an overview is provided for each identified threat.

Procedure

Click "Knowledge Base" tab in the Main Menu

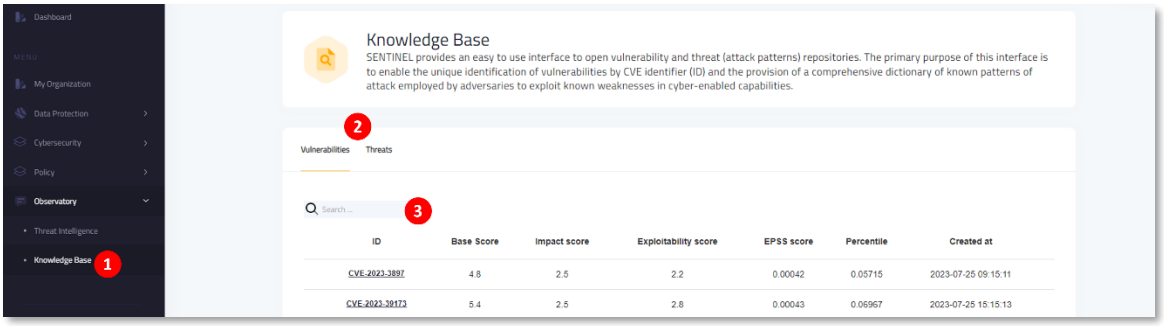
Select either ‘’Vulnerabilities’’ or ‘’Threats’’ tab

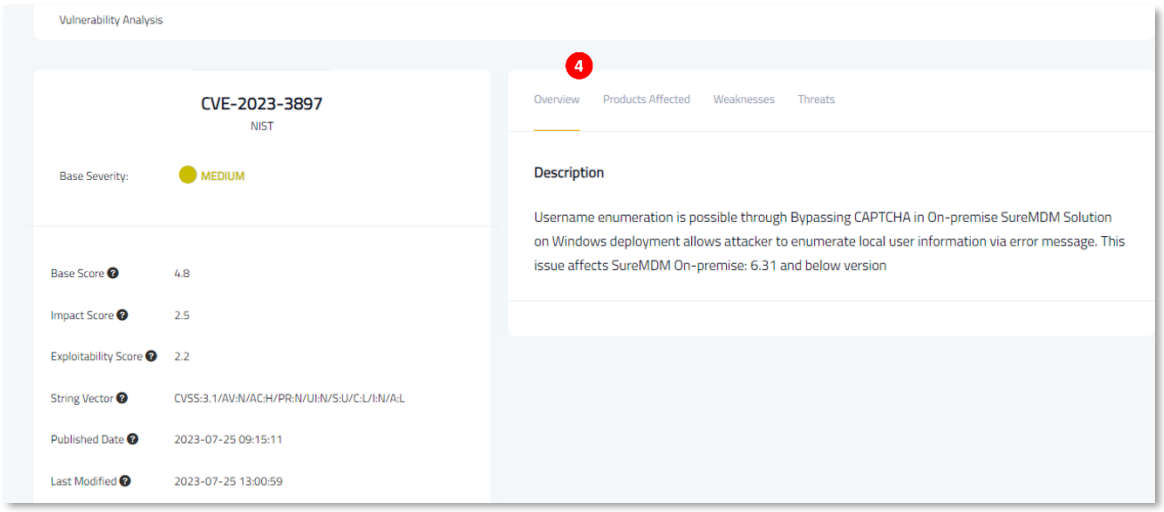
Vulnerabilities tab: Browse through vulnerability IDs or search a specific ID from the Search filter

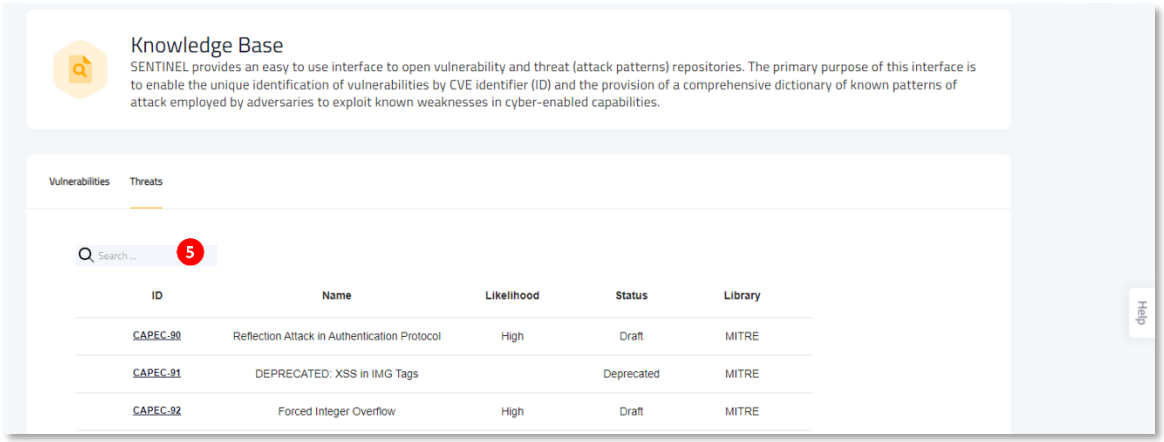
On the landing page of each vulnerability, the base severity is provided alongside with other relevant information. You can click on the vulnerability overview, products affected, weaknesses and threats tabs

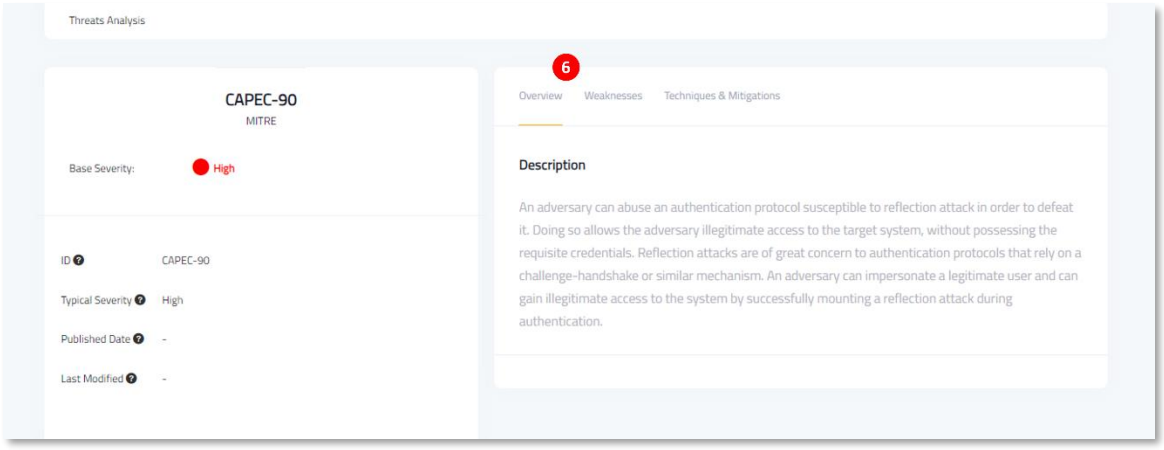
Threats tab: Browse through threat IDs or search a specific ID from the Search filter. Name, likelihood, status and threats library are provided on the same page.

Click on a specific threat ID for a detailed description of it









9. Receive Security Notifications

Finally, if you have installed and integrated a compatible cybersecurity infrastructure monitoring plugin, such as Security Infusion, you will be able to receive security notifications.

The SENTINEL Notification center receives reported events, which are identified by Security Infusion plugin, by the Notification Aggregator module

Receive Security Notifications

Procedure

Click on the Bell button on the top right corner of every page in the platform, which turns orange whenever there is a new notification that the user needs to be made aware of

Click Refresh button just below the Bell, which the user can click in order to update the notifications manually

Appendix -III: NDA Template

NON-DISCLOSURE AGREEMENT

THIS AGREEMENT dated **XX/XX/2023** by and between the parties hereto:

ON THE FIRST PART

1. The Enterprise under the corporate name **……,** legally represented for the signing hereof by ....., hereinafter referred to, for the sake of brevity, as **"the Disclosing Party"**, and,

ON THE SECOND PART

2. INFORMATION TECHNOLOGY FOR MARKET LEADERSHIP (**ITML**), represented by the Project Coordinator Dr George Bravos acting on its behalf and on behalf of the beneficiaries in the EU-funded project SENTINEL, based on the Consortium Agreement that was signed in April 2021.

The Consortium beneficiaries hereinafter each referred to as "**Recipient**" or collectively referred to as the "**Recipients**"

WHEREAS

A. the **Disclosing Party** and the **Recipients** for the purpose of establishing a cooperative relationship, conducting piloting activities and pursuant to the research related to the SENTINEL project anticipate that the **Disclosing Party** may disclose or deliver to **Recipients** information relating to its administration, management, transactions, activity and operation in general.

B. In the course of its business, the **Disclosing Party** pays particular attention to the confidentiality of the information provided thereby or the information disclosed to its **Recipients** and wishes to reasonably protect data and information relating to its administration, management, transactions, activity and operation in general, to prevent them from being communicated or disclosed to unauthorised third parties.

C. In view of the foregoing, the parties wish to conclude this agreement.

IN CONSIDERATION OF THE ABOVE

It has been agreed upon, stipulated and mutually accepted as follows:

1. Confidential Information

For the purposes of this agreement, the term "Confidential Information", wherever found hereafter in this agreement, will have the following meaning:

All information and data which will be provided by the **Disclosing Party** to the **Recipients** and/or of which the **Recipients** will become aware regarding the management, administration, operation, business organisation, investments, transactions, business partners, shareholders or members thereof, products, services, financial status, customers, principals, suppliers, business policy, business plans and strategies, practices, programmes, production methods, know-how, systems, processes and techniques of sales and marketing, pricing, purchases, supplies, etc. of the **Disclosing Party**, which are not known to third parties, excluding information that is publicly known or has been published or announced or disclosed without the **Recipients**' involvement. The aforementioned Confidential Information may be contained on any media, whether electronic or otherwise, without necessarily being marked "confidential".

2. Entry into force

This agreement shall enter into force and shall take effect as of the date of its signing and shall expire on 31/05/2024. The obligations to keep Confidential Information confidential pursuant to this Agreement shall remain valid for the **Recipients** even after the end of this Agreement for a period of four (4) years thereafter.

3. Obligations of the Recipients

3.1. The **Recipients** undertakes not to disclose, publish, distribute or otherwise disclose to any third party any of the Confidential Information otherwise than for the purpose for which it was disclosed.

3.2. The **Recipients** undertake to take reasonable care so that any Confidential Information collected and stored as part of the SENTINEL project be kept in a secure environment to prevent the risk of loss or access by third parties.

3.3. The **Recipients** shall use the Confidential Information exclusively for the purpose of the SENTINEL project and ensure that internal distribution of Confidential Information by a **Recipient** shall take place on a strict need-to-know basis only.

3.4. The **Recipients** undertake to immediately notify the **Disclosing Party** of any loss or unauthorised disclosure or use of the Confidential Information of which he may become aware.

3.5. All **Recipients** obligations arising out of this Non-Disclosure Agreement relating to Confidential Information shall apply to and bind the **Recipients** vis-à-vis **Disclosing Party**, its subsidiaries, beneficiaries and affiliate undertakings or undertakings that are jointly controlled with the **Disclosing Party**, as well as its clients, principals, Beneficiaries and **Disclosing Party**'s business partners in general.

4. Breach of the non-disclosure obligation

4.1. In the event of a fault-based breach of the **Recipients**' non-disclosure obligation, the **Recipients** shall be obliged, first, to cease the breach without delay and to desist in the future, and second, to remedy any direct loss suffered by the **Disclosing Party** for that reason.

4.2. The **Recipients** will not be held liable for any breach of for the disclosure, announcement and communication in general of Confidential Information to third parties:

- where it is required by law, a court decision, an act or decision of any public entity or authority, after having advised the **Disclosing Party** in advance and in writing, and
- where the Confidential Information is already or becomes known to third parties, or to the general public, or announced or becomes public knowledge without the **Recipients**' fault.

5. Final Provisions

5.1. Any amendment to the terms of this agreement shall be made and evidenced only in writing, expressly excluding any other means of proof, including the oath.

5.2. This agreement is governed by the Greek substantive and procedural law, whilst the Courts of Athens shall be exclusively competent to resolve any dispute arising between the parties

under this agreement, in particular regarding the conclusion, performance and interpretation thereof.

In witness of the aforementioned understandings between the parties, this agreement has been drawn up and, after being read and witnessed by the parties, is signed the time specified below.

THE PARTIES

On behalf of the Company	On behalf of the SENTINEL Project
Date:	Date:
Name and Surname Signature:	Name and Surname Signature: