SENTINEL

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

D5.2 - The SENTINEL visualisation and UI component - second version

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

Project Information

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

Document Information

Work Package	**Work Package - 5**
Deliverable Title	D5.2 - The SENTINEL visualisation and UI component - second version
Version	1.4
Date of Submission	30/11/2022
Main Editor(s)	Marinos Tsantekidis (AEGIS)
Contributor(s)	Kostas Bouklas (ITML)
Reviewer(s)	Anna Maria Anaxagorou (ITML), Manolis Falelakis (INTRA)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	27/09/2022	ToC shared	Confidential
1.1	17/10/2022	Updated ToC and input provided for Sections 1, 2 and 3	Confidential
1.2	14/11/2022	Input collected for Sections 4.1, 4.2, 4.3, 4.4, 4.5, 4.6 and 4.7	Confidential
1.3	22/11/2022	Final input and release for internal review	Confidential
1.4	29/11/2022	Final version after review comment	Public

Table of Contents

List of Figures

Abbreviations

Abbreviation	**Explanation**
CS	CyberSecurity
CSS	Cascading Style Sheets
DoA	Description of Action
DPIA	Data Protection Impact Assessment
FVT	Forensics Visualization Toolkit
GA	Grant Agreement
GDPRC	General Data Protection Regulation Compliance
HTTPS	HyperText Transfer Protocol Secure
HTML5	HyperText Markup Language 5
IdMS	Identity Management System
KB	Knowledge Base
MISP	Malware Information Sharing Platform
MVP	Minimum Viable Product
OTM	Organizational Technical Measure
PA	Processing Activity
PDP	Personal Data Protection
ROPA	Record of Processing Activity
SME	Small Medium Enterprise
SSO	Single Sign-On
UC	Use Case
UI	User Interface
WP	Work Package

Executive Summary

D5.2 "The SENTINEL visualisation and UI component – second version" is one of the outcomes of *Work Package (WP) 5 (SENTINEL continuous integration and system validation)* of the SENTINEL Project and more specifically *Task 5.1 (Interactive visualisations and front-end components)*. This task is focused on the development and the implementation of the interactive visualisation toolkit, and UI framework of the SENTINEL platform.

This document gives an updated and more detailed view of the MySentinel UI dashboard in the first complete prototype of the platform, after being updated since the MVP release. More specifically it describes on the necessary functions developed and implemented to act as a user-friendly and intuitive public-facing platform. Furthermore, it serves as a bridge to all data interchanged between the components developed in "WP2 - The SENTINEL privacy and personal data protection technologies" and "WP3 - The SENTINEL digital core" and related to the services deployed in "WP4 - The SENTINEL services".

This document is preceded by its first version *"D5.1 - The SENTINEL visualisation and UI component – first version"* and it will be complimented in the future by its subsequent third and last version "*D5.3 - The SENTINEL visualisation and UI component – final version"* by giving complete overview of the SENTINEL front-end components integrated with MySentinel UI dashboard.

1 Introduction

The SENTINEL visualisation/UI component and the primary dashboard of the platform is MySentinel. It aggregates data from all front-end components and user-facing web applications. It welcomes new and existing end-users and provides quick visual insight into SMEs' current progress and score, by presenting every connected service. Furthermore, it offers a set of front-end modules that provide corresponding interactions between the user and SENTINEL's services. Based on the detailed information that can be found in deliverable "*D1.2 – The SENTINEL technical architecture* (Section 4)", this set comprises the following:

- **Self-Assessment Centre**: provides access to all self-assessment plugins that SENTINEL offers.
- **Policy Enforcement Centre**: provides access to informative tables, charts and color-coded alerts from which the user will be able to select which policy points to see according to their own needs.
- **Compliance Centre**: provides access to advanced visualisations that allow monitoring of the data privacy legislation compliance, while it carefully selects and crafts informative guidelines.
- **Security Notifications**: provides access to live notification alerts and key characteristics of the monitored systems and operations through advanced visualisations.
- **Incident Reporting Centre**: gives end-users the opportunity to manually submit observed incidents that occur within the context of their business operations and share them to external sources, in anonymised manner.
- **Observatory**: provides access to a broad knowledge base for cybersecurity and privacy with which the user is able to exchange real-time data among open security platforms globally.

The previous version of this deliverable "*D5.1 – The SENTINEL visualisation and UI component – first version*" is part of the MVP release of the platform, where only components and modules that are necessary for a subset of the overall seven (7) use-cases listed in deliverable D1.2 – Section 2.3 were developed and took part in the platform. Specifically, these use-cases are (the numbering follows the one stated in D1.2):

1. **SME registration and profiling:** The SME representative registers the company[1] and fills in the related questionnaire. Based on this information, the system provides a profile of the company.
2. **Completing a self-assessment workflow:** The user completes a self-assessment workflow that has been proposed by the SENTINEL platform, after gathering the SME requirements during registration.

[1] The terms "company" and "organization" are interchangeable.

3. **Acquiring policy recommendations:** The SME representative fills out the company security profile and performs related self-assessment tasks indicated by the system. Then they receive a tailor-made set of security policies.

6. **Consulting the Observatory Knowledge Base (KB):** The SME representative browses the SENTINEL Observatory KB and accesses information about recently identified data and privacy breaches. The KB is continuously updated and synchronised with external resources.

For this version of the platform – the first complete prototype, the components and modules that are necessary for the remaining use-cases are developed and included. Specifically, these use-cases are (the numbering follows the one stated in D1.2):

4. **Receiving security notifications:** The system detects a CS or PDP incident that affects an SME and alerts the SME representative to attend to it.

5. **Policy enforcement monitoring:** The SME representative provides an update to the system concerning the status of implementation of policies they have received as recommendations from the SENTINEL platform.

7. **Incident reporting and sharing:** A security incident has been detected and the SME wants to report and share it with appropriate response teams and/or open security data platforms, such as malware information sharing and incident response hubs.

Consequently, the dashboard is now complete with the links and user experience flow that correspond to all use-cases and accompanying modules. This means that, taking into consideration the revised architecture of the SENTINEL platform presented in deliverable D1.2 (Figure 1), apart from the MySentinel dashboard, the Self-Assessment Centre and the Observatory modules and interconnected parts of the respective contexts included in the MVP release, most of the remaining modules (Policy Enforcement Centre, Security Notification and Incident Reporting Centre) and relevant parts of the respective contexts are also included in this second version of the platform.

The work presented in this deliverable is part of the integrated solution and thus the UI interaction and integration with other contexts within the first complete prototype use-cases is explained in D5.5 with more detail.

The communication from and towards the dashboard is encrypted and the web application is served over HTTPS. Within the application, all SENTINEL modules are presented as options relevant to the use cases. The user is able to get insights into current progress and score, while advanced and intuitive visualisations are available on each service's dedicated dashboard.

Technologies

So far, the development of the platform has been based on a number of widely used technologies. We continue to rely on these in order to deliver seamless integration of all platform modules. MySentinel is based upon Metronic (version 8)[2], a template built with:

[2] https://keenthemes.com/metronic/

- Angular, a free and open-source web application framework (version 12 used in Metronic)[3] and
- Bootstrap, a free and open-source CSS framework aimed at responsive, front-end web development to support different resolutions and devices, containing HTML5, CSS3 and JavaScript-based design templates (version 5 used in Metronic)[4].

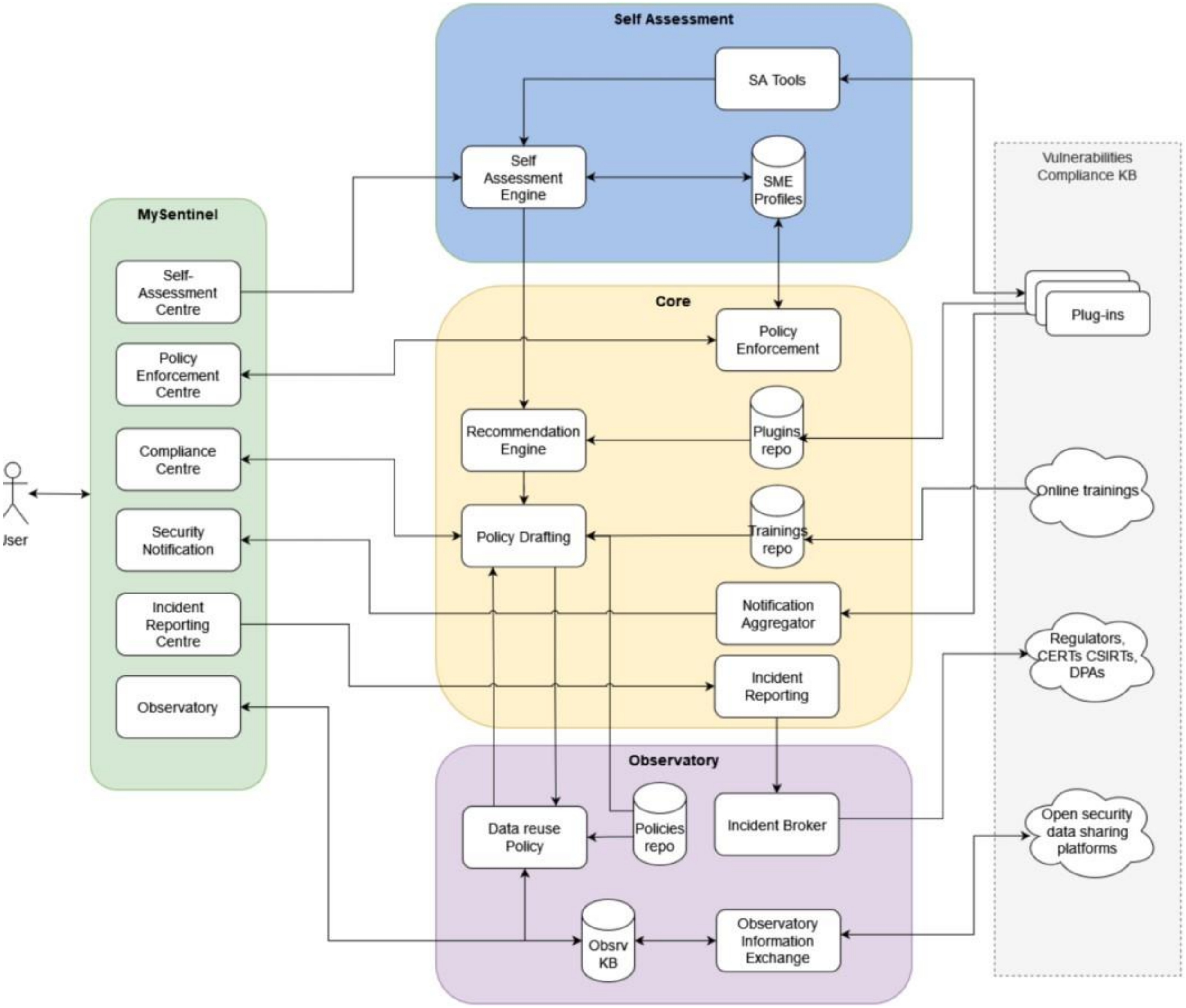


Figure 1. Overall revised architecture of the SENTINEL platform

Additionally, we use Keycloak[5], which has been integrated with the UI to provide SSO services: authentication and authorization for SME representatives/end-users. Keycloak is an open source software product that provides SSO with Identity and Access Management, allowing users to be logged in (or out) only once, at a central point and then be able to use the whole array of SENTINEL services. The platform's Keycloak infrastructure is offered by ITML. It stores the user's credentials in a secure way and allows them to sign-in to the UI, but also to external plugins such

[3] https://angular.io/
[4] https://getbootstrap.com/
[5] https://www.keycloak.org/

as CyberRange. When the user navigates to MySentinel, they are redirected to the infrastructure's login page, where they are asked to enter their credentials (username and password). Upon successful authentication, they are redirected back to the main MySentinel Dashboard. More details about Keycloak can be found in deliverable D2.2.

1.1 Purpose of the document

Similarly, to D5.1, Deliverable D5.2 is a demonstrator thus its main purpose is to showcase the SENTINEL platform's UI. This includes all interconnections of SENTINEL's several modules and components with the front-end, in a number of use cases. This document presents the visualization and UI component (MySentinel) of the first complete prototype, including screenshots taken directly from the developed website that show the action flow an end-user needs to follow in order to complete a number of actions required by specific scenarios. The deliverable provides support to the following objective:

Objective 1 of the DoA *"Develop and support an end-to-end digital Privacy and Personal Data Protection (PDP) compliance framework and Identity Management System (IdMS) that enables Speed, Flexibility, Quality, Efficiency and Security for SMEs/MEs. Validate, demonstrate, and carry out experimental evaluation of the proposed framework in real-world SMEs/MEs operation scenarios."* and specifically the set target of increasing acceptance of SENTINEL solutions based on the given UI.

Objective 4 of the Description of Action (DoA) *"Facilitate an efficient exploration of cost-efficient, intelligent and automated PDP compliance and Identity Management full potential in SMEs/MEs environments and realise societal and economic opportunities by validating SENTINEL framework in real-world settings via use cases driven by complementary industries".* In particular, this deliverable addresses the construction of an informative mechanism for both data analysts and non-IT experts of SMEs/MEs.

1.2 Structure of the document

The rest of the document is organized as follows:

- *Section 2* presents the interdependencies among the various tasks, along with their leaders.
- *Section 3* presents the sitemap of the MySentinel UI, with the association of each part of it with a specific use-case.
- *Section 4* describes the individual menu items and accompanied with screenshots from the actual web platform.
- *Section 5* concludes this document.

1.3 Intended readership

This document is a public document that accompanies the public demonstrator for the SENTINEL's platform UI. It is intended for both consortium members and external to the project stakeholders, since it shows the public-facing website of the platform, which an end user can access as a member of an SME and perform all activities that SENTINEL has to offer. Additionally, as this document presents and explains all important interactions of the user with the UI for the first complete prototype, it may serve as a user manual for the end-users and testers of the SENTINEL framework.

1.4 Updates since D5.1

Deliverable D5.1 includes details about the MySentinel UI in the MVP phase of the platform. In deliverable D5.2, we update those details and provide information about the UI of the first complete prototype of the platform. Summarizing the updates, we:

- Update the interconnections of the MySentinel context with the other contexts of the platform.
- Provide the additional use-cases included in this version.
- Update the sitemap of MySentinel to show the associated pages of the newly added menu items that correspond to these additional use-cases.
- Provide information about these menu items accompanied by screenshots that show the corresponding functionalities and by references to the latest version of the relevant deliverables.

2 Task Interdependencies

Naturally, the UI communicates with the other parts of the platform. Each specific dashboard component (e.g., Policy Enforcement Centre, Incident Reporting Centre) interconnects with its counterpart in the respective context. Every party in this two-way communication corresponds to a specific Task, as described in the DoA of the project's Grant Agreement (GA). Figure 2 shows these interdependencies.

In the previous version of this deliverable that reports on the MVP release (D5.1), we show how the MySentinel context is interconnected with the Self-Assessment Engine (T4.3 – IDIR). By extension, it also communicates with the Self-Assessment Tools (T2.1 – LIST) and the SME profiles repository (T4.2 – STS). More information about these can be found in deliverables D2.1 and D4.1, respectively. Additionally, it is connected with the Observatory context and more specifically its Knowledge Base (T4.4 – ITML) and Information Exchange (T3.1 – AEGIS) modules, with more details available in deliverables D3.1 and D4.1.

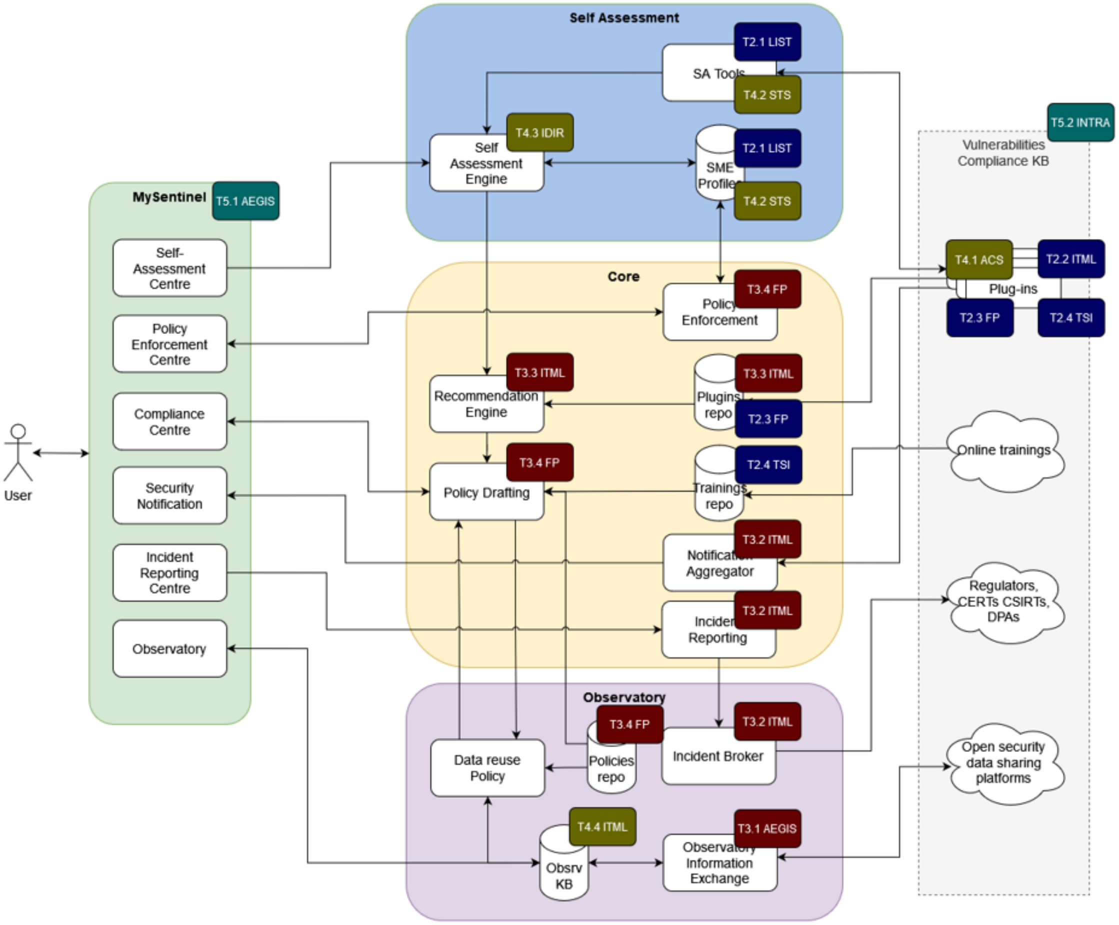


Figure 2. Task interdependencies and leaders

In the current version of the platform – the first complete prototype, most of the remaining interconnections have been implemented. The MySentinel context is connected with the Core context, with specific dashboard components interacting with the respective modules in the Core:

- the Policy Enforcement Centre with the Policy Enforcement module (T3.4 – FP)
- the Security Notification with the Notification Aggregator (T3.2 – ITML)
- the Incident Reporting Centre with the Incident Reporting module (T3.2 – ITML)

More information about these can be found in deliverables D2.2 and D3.2.

3 Sitemap

As mentioned in the Introduction, in the MVP version the MySentinel UI includes only menu item links that correspond to modules needed to implement the four use cases of the MVP. Figure 3 presents the sitemap of the front-end, showing the site's structure, the hierarchy of the different pages on the platform and how these are interlinked. Information is organized in such a way so as to facilitate easy navigation for end users.

Furthermore, in Figure 3, the several parts of the UI are associated with the use cases included in the MVP. Specifically:

UC1 → My Organization (Profile, Contacts, Assets Profile, Processing Activities)

UC2 → Self-Assessment (DPIA, GDPRC, Simulation Environment, Cyber Range)

UC3 → Policy (Recommendations)

UC6 → Observatory (Knowledge Base)

The Processing Activities of an organization are part of its profile in the platform. Additionally, the two types of Self-Assessment (DPIA, GDPRC) are performed for each PA separately. Consequently, the "Processing Activities" section of the UI is associated with two use cases (UC1, UC2).

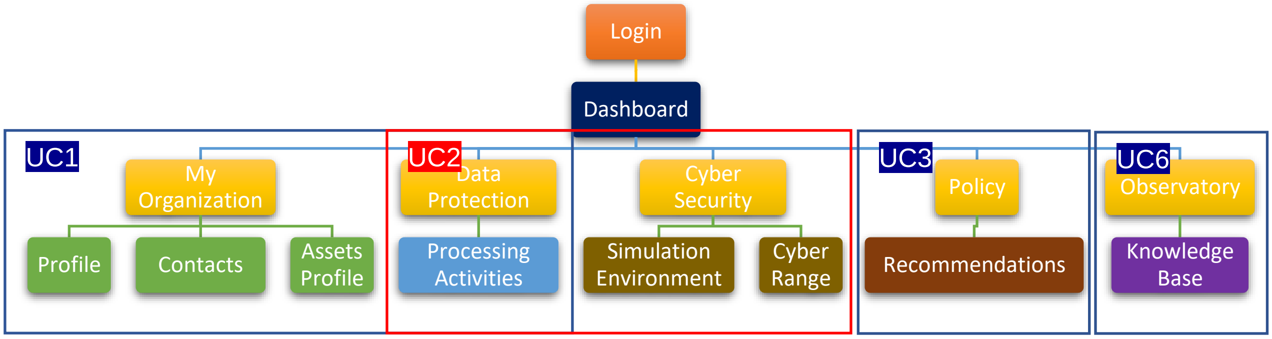


Figure 3. MySentinel sitemap in the MVP

In the first complete prototype of the platform – the current version, the rest of the use-cases have been included in the platform. Overall, the use-cases associated with the updated version are:

UC1 → My Organization (Profile, Contact persons, Generic asset profile, Asset inventory Processing Activities, ROPA)

UC2 → Self-Assessment (Processing Activities, ROPA, Assets, Measures, Simulation Environment, Cyber Range, FVT)

UC3/UC5 → Policy (Recommendations)

UC4 → Security Notifications

UC6/ UC7 → Observatory (Knowledge Base)

Figures Figure 4, Figure 5, Figure 6, Figure 7 and Figure 8 present the updated sitemap of the front-end. For the sake of clarity and space, we present several instances of the sitemap based on the use-cases with which the several parts of the UI are associated.

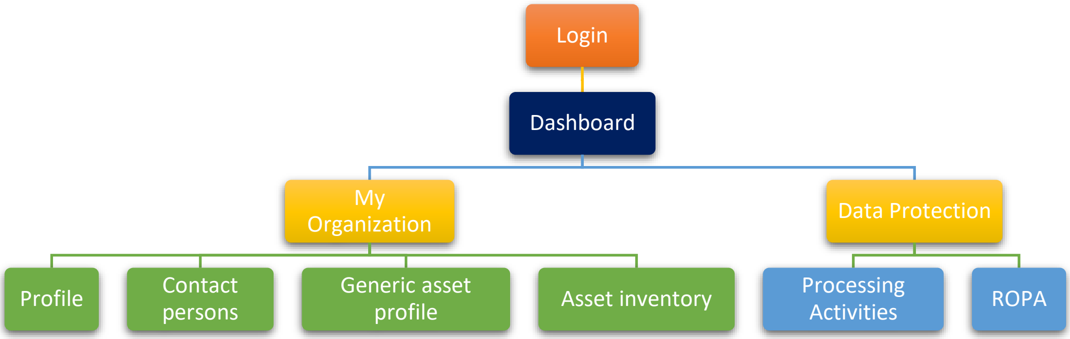


Figure 4. MySentinel sitemap associated with UC1

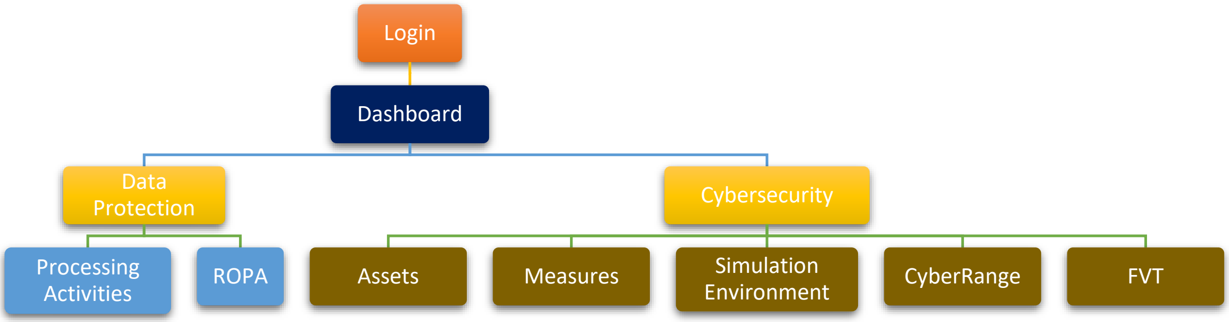


Figure 5. MySentinel sitemap associated with UC2

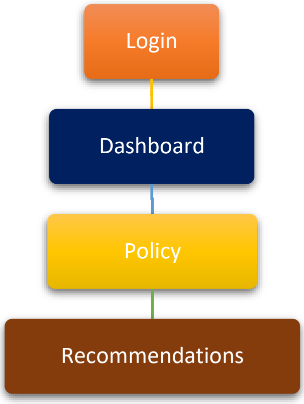


Figure 6. MySentinel sitemap associated with UC3 and UC5

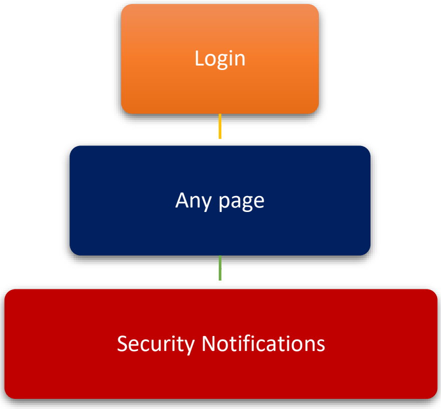


Figure 7. MySentinel sitemap associated with UC4

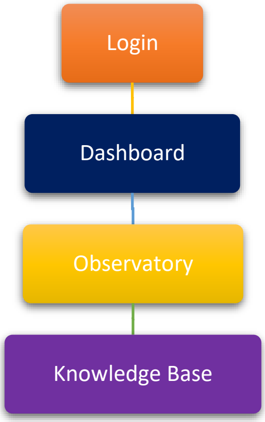


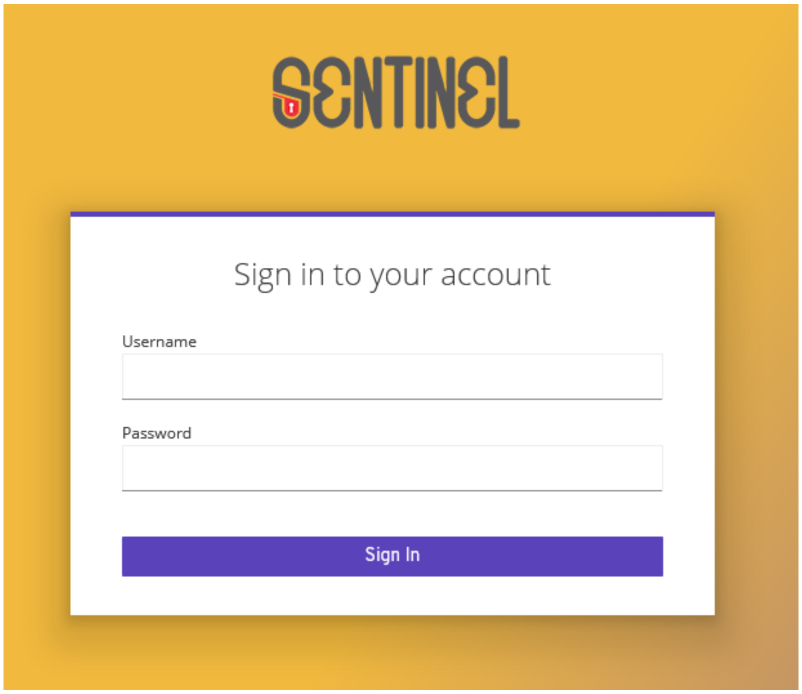
Figure 8. MySentinel sitemap associated with UC6 and UC7

4 Menu Items and Screenshots

In this section, we explain all menu items (both included in the previous version as reported in D5.1, as well as in this updated current version) and associated pages and provide screenshots that show the corresponding functionalities.

4.1 Login page

When a user first visits the SENTINEL platform, they are redirected to the login page (Figure 9), where they are prompted to enter their credentials (username, password), in order to sign in to their account.



SENTINEL

Sign in to your account

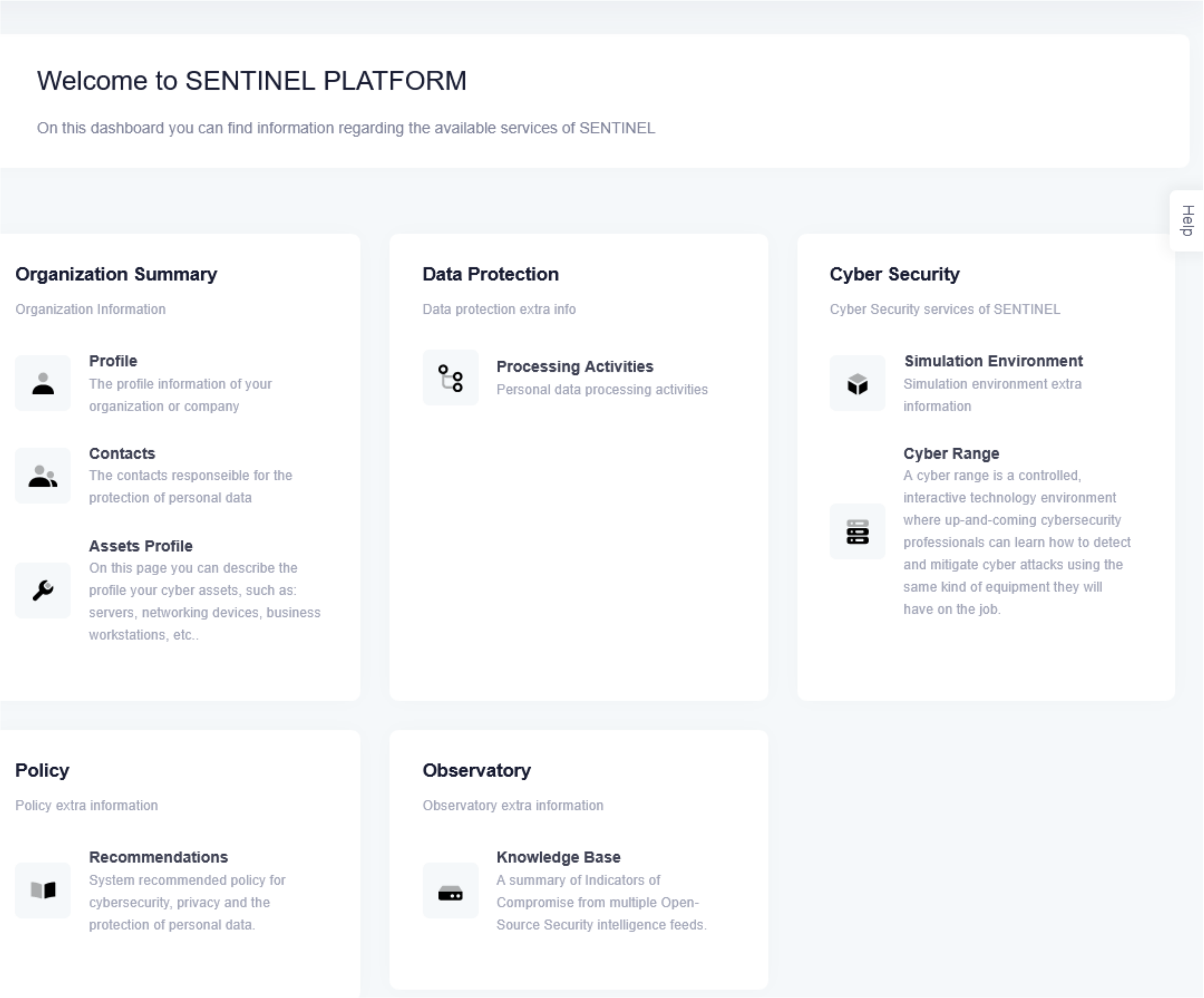
Username

Password

Figure 9. SENTINEL login page

4.2 Dashboard

By clicking either the SENTINEL logo or the “Dashboard” menu item link on the top left, the user ends up in the initial dashboard of the platform (as shown in Figure 10). There, they can find information explaining what every link corresponds to and what they can expect to perform when visiting each section. This is an initial entry page that we offer to the end user, so that they can get acquainted with the platform and easily explore the offered functionalities from a single page.



Welcome to SENTINEL PLATFORM

On this dashboard you can find information regarding the available services of SENTINEL

Organization Summary

Organization Information

Profile
The profile information of your organization or company

Contacts
The contacts responseible for the protection of personal data

Assets Profile
On this page you can describe the profile your cyber assets, such as: servers, networking devices, business workstations, etc..

Data Protection

Data protection extra info

Processing Activities
Personal data processing activities

Cyber Security

Cyber Security services of SENTINEL

Simulation Environment
Simulation environment extra information

Cyber Range
A cyber range is a controlled, interactive technology environment where up-and-coming cybersecurity professionals can learn how to detect and mitigate cyber attacks using the same kind of equipment they will have on the job.

Policy

Policy extra information

Recommendations
System recommended policy for cybersecurity, privacy and the protection of personal data.

Observatory

Observatory extra information

Knowledge Base
A summary of Indicators of Compromise from multiple Open-Source Security intelligence feeds.

Figure 10. SENTINEL Dashboard

4.3 My Organization

By clicking on this menu item link (Figure 11), the user is presented with a page containing the four corresponding tabs, as shown in Figure 18. It includes the “Profile” tab, as before. The “Assets profile” tab has been renamed to “Generic asset profile”. The “Contacts” tab has been renamed to “Contact persons”. The extra tab “Asset inventory” has been added.

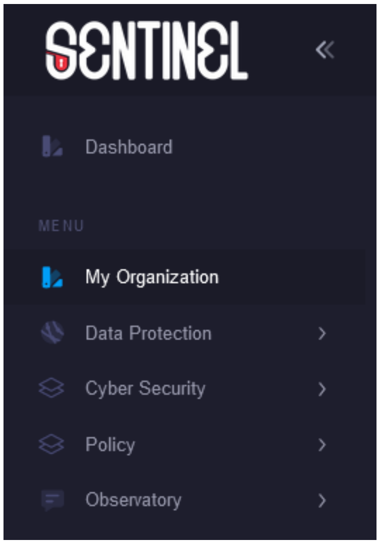


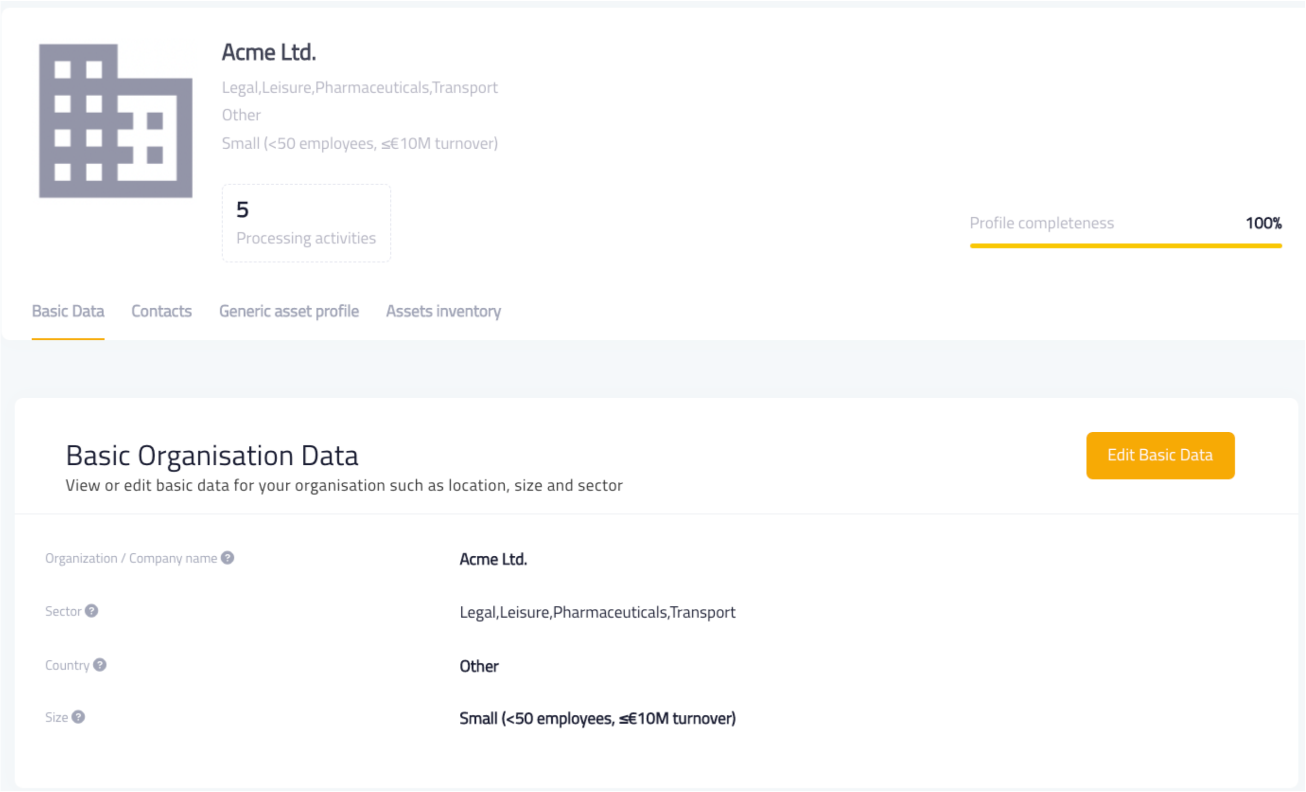
Figure 11. My Organization menu item

4.3.1 Basic Data

In Figure 12, the organization profile view page is depicted. The user can see the data they have previously saved in their organization's profile, namely:

- Organization/Company name
- Sector
- Country
- Size

There is also an "Edit Basic Data" button that allows them to edit these details, which leads to the page depicted in Figure 19Figure 13. The user can, then, type in their company's name and select the sector in which it is active, its country and its size. These selections are performed from the respective dropdown lists that are populated with predefined options. The "Save" button stores all the changes in the organization's profile, while the "Cancel" button reverts all the changes and returns to the view page.



Acme Ltd.

Legal,Leisure,Pharmaceuticals,Transport

Other

Small (<50 employees, ≤€10M turnover)

5
Processing activities

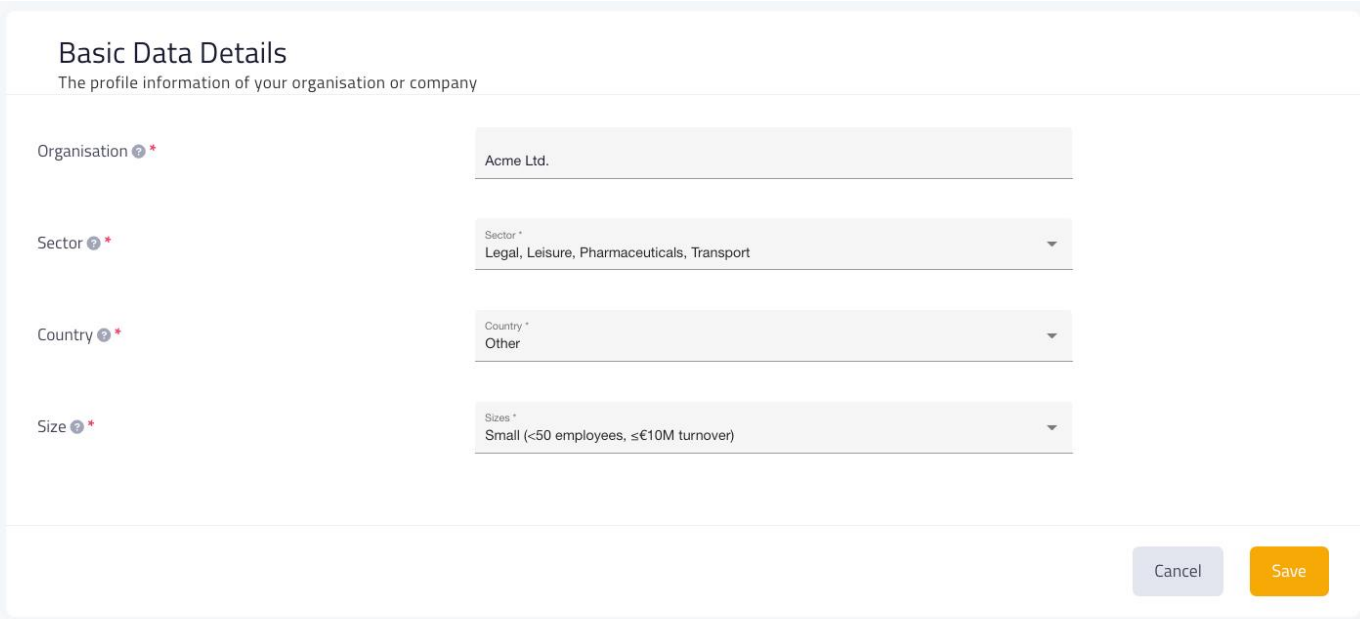
Profile completeness 100%

Basic Organisation Data

View or edit basic data for your organisation such as location, size and sector

Organization / Company name	Acme Ltd.
Sector	Legal,Leisure,Pharmaceuticals,Transport
Country	Other
Size	Small (<50 employees, ≤€10M turnover)

Figure 12. My Organization - Profile view page



Basic Data Details

The profile information of your organisation or company

Organisation *	Acme Ltd.
Sector *	Sector * Legal, Leisure, Pharmaceuticals, Transport
Country *	Country * Other
Size *	Sizes * Small (<50 employees, ≤€10M turnover)

Figure 13. My Organization - Profile edit page

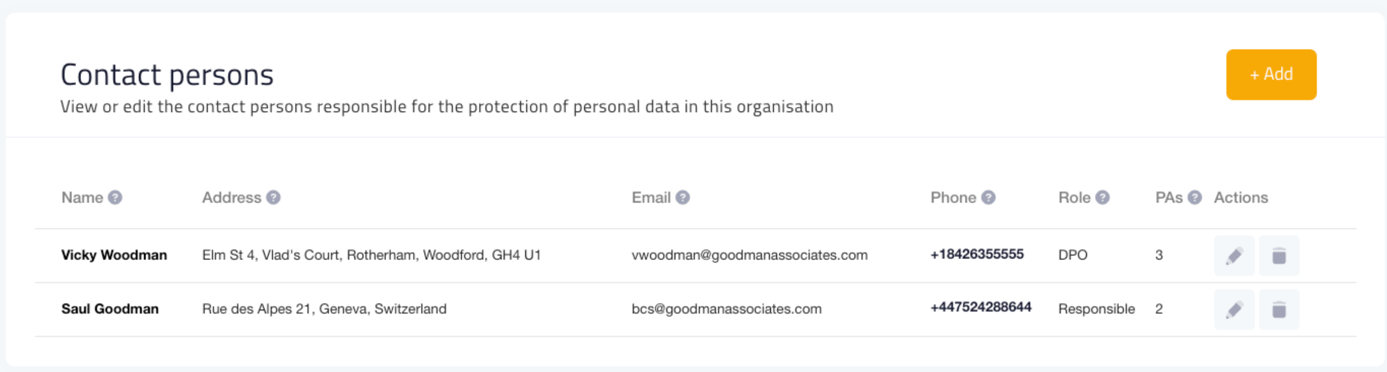
4.3.2 Contact persons

On this tab, the user can see the complete list of GDPR contact persons that are members of the specific organization. There are columns for their Name, Address, E-mail, Phone number and their Role within the organization. Additionally, there are two more columns:

a) PAs – Processing Activities: This is filled in automatically, by collecting all the PA IDs that the specific person is connected with.

b) Actions: Buttons that the user can click, to perform additional actions, i.e., “Edit” (the Pencil icon) and “Delete” (the Rubbish Bin icon) a specific record.

This page can be seen in Figure 14.



Contact persons

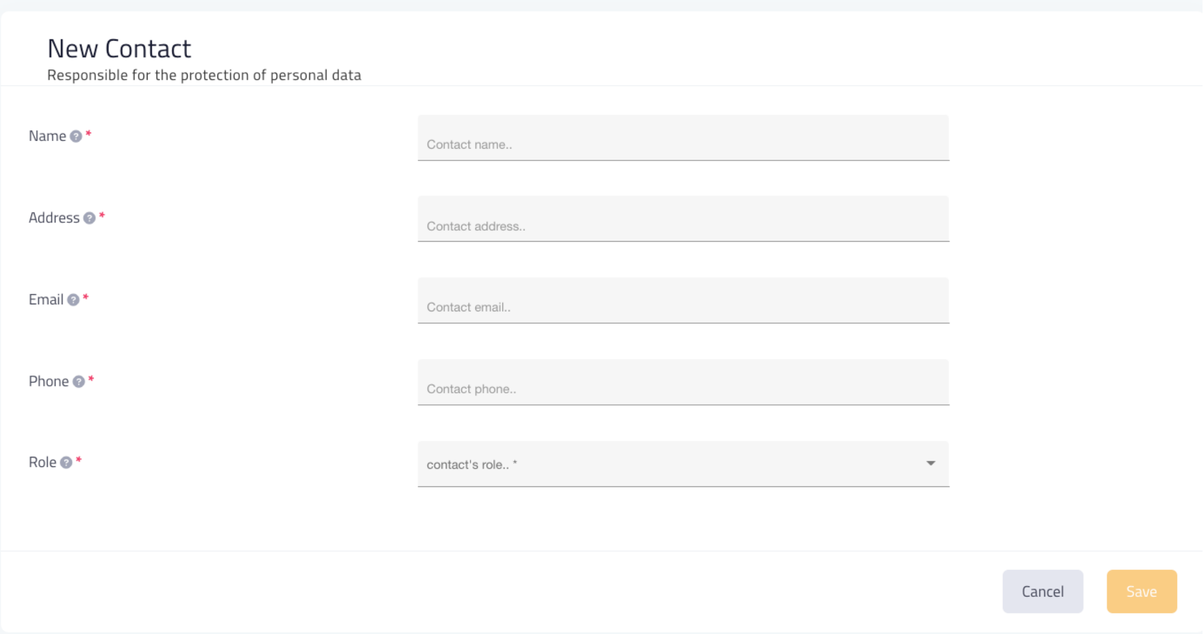
View or edit the contact persons responsible for the protection of personal data in this organisation

Name ?	Address ?	Email ?	Phone ?	Role ?	PAs ?	Actions
Vicky Woodman	Elm St 4, Vlad's Court, Rotherham, Woodford, GH4 U1	vwoodman@goodmanassociates.com	**+18426355555**	DPO	3	✎ 🗑
Saul Goodman	Rue des Alpes 21, Geneva, Switzerland	bcs@goodmanassociates.com	**+447524288644**	Responsible	2	✎ 🗑

Figure 14. My Organization - Contact persons page

By clicking the “Add” button the user has the ability to add a new contact person for their company, by entering data in the respective fields of the form and then clicking the “Save Changes” button. They can also revert all the changes and return to the view page by clicking the “Cancel” button (Figure 15).

After adding a contact, a new row containing all its data is added in the table in Figure 14.



New Contact

Responsible for the protection of personal data

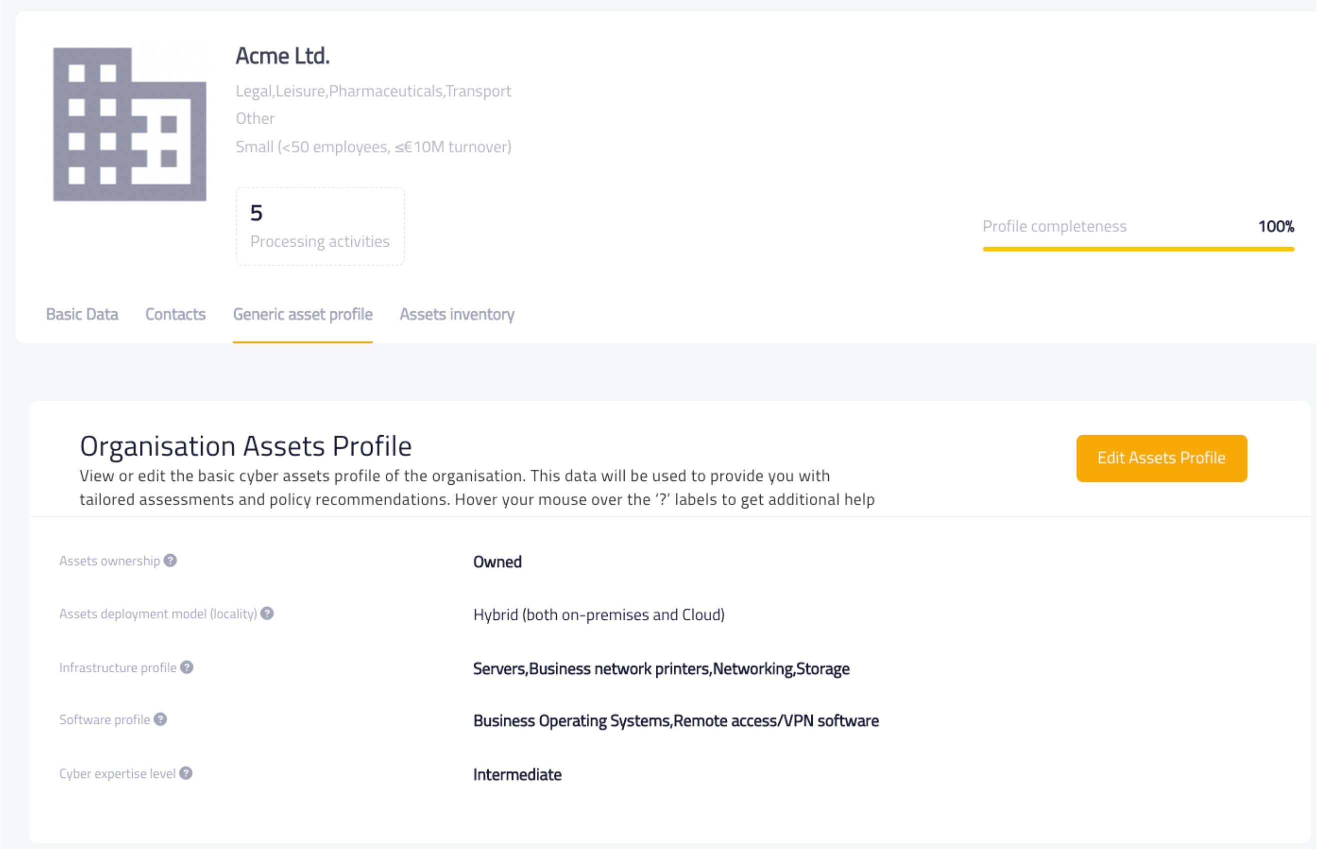
Name *	Contact name..
Address *	Contact address..
Email *	Contact email..
Phone *	Contact phone..
Role *	contact's role.. *

Figure 15. My Organization - Add Contact page

4.3.3 Generic asset profile

In this part of the platform, the user can see/edit the details about the profile of the assets that the organization uses, as can be seen in Figure 16. The fields are:

- Assets ownership: Whether the assets are owned or not.
- Assets deployment model: If they are on-premises, in the cloud or both.
- Infrastructure profile: What kind of assets (servers, workstations, networking devices, etc.).
- Software profile: What kind of software (Operating Systems, Business Applications, etc.).
- Cybersecurity expertise level: Refers to the responsible persons inside the organization.



Acme Ltd.

Legal,Leisure,Pharmaceuticals,Transport

Other

Small (<50 employees, ≤€10M turnover)

5 Processing activities

Profile completeness 100%

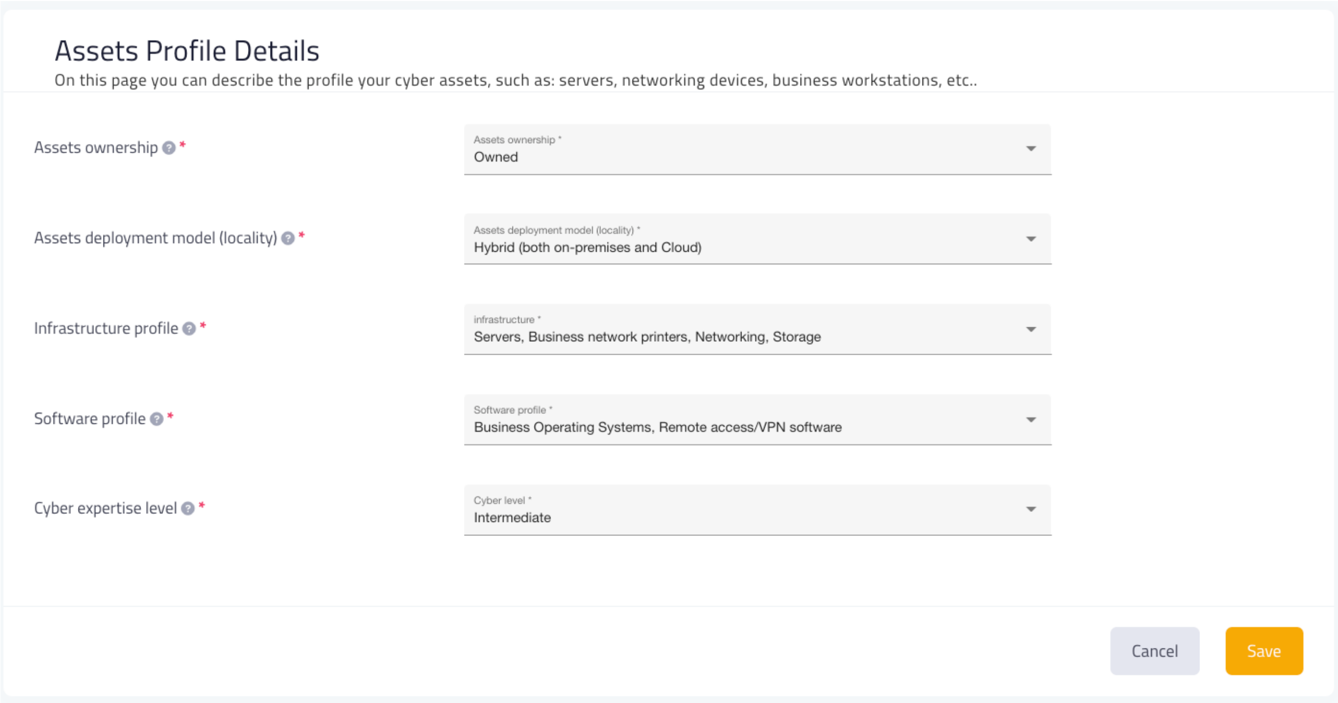
Organisation Assets Profile

View or edit the basic cyber assets profile of the organisation. This data will be used to provide you with tailored assessments and policy recommendations. Hover your mouse over the '?' labels to get additional help

Assets ownership ?	Owned
Assets deployment model (locality) ?	Hybrid (both on-premises and Cloud)
Infrastructure profile ?	Servers,Business network printers,Networking,Storage
Software profile ?	Business Operating Systems,Remote access/VPN software
Cyber expertise level ?	Intermediate

Figure 16. My Organization – Generic asset profile view page

By clicking on the “Edit Assets Profile” button, the user is presented with the corresponding edit page, as depicted in Figure 17, which follows the logic behind the organization’s profile edit page (Figure 13).



Assets Profile Details

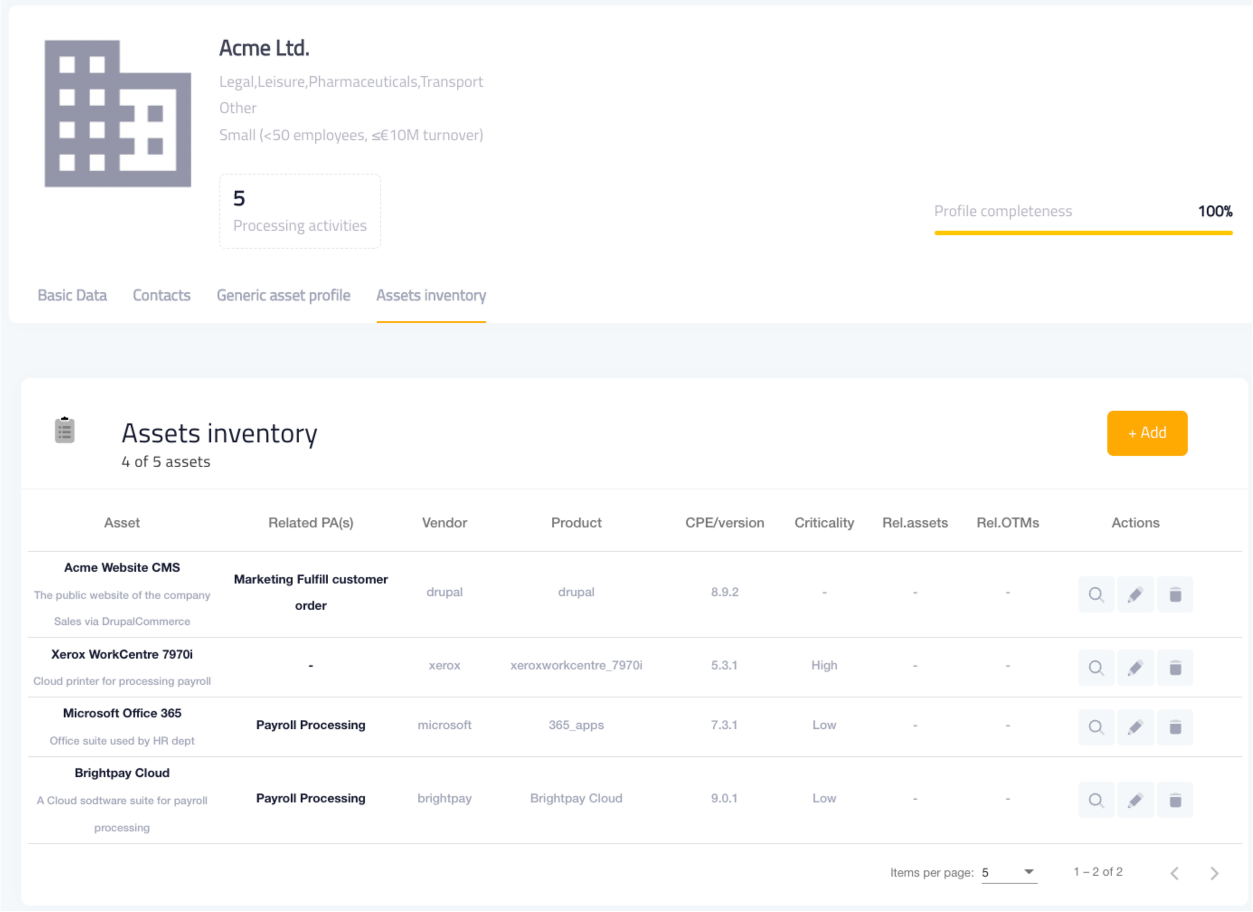
On this page you can describe the profile your cyber assets, such as: servers, networking devices, business workstations, etc..

Assets ownership *	Assets ownership * Owned
Assets deployment model (locality) *	Assets deployment model (locality) * Hybrid (both on-premises and Cloud)
Infrastructure profile *	infrastructure * Servers, Business network printers, Networking, Storage
Software profile *	Software profile * Business Operating Systems, Remote access/VPN software
Cyber expertise level *	Cyber level * Intermediate

Figure 17. My Organization - Generic asset profile edit page

4.3.4 Asset inventory

This tab is a new addition to the platform (Figure 18). It lists all the assets of the organization, some of which may not be related to a PA. For example, in the figure below we can see four assets in the specific organization, however only three are related to a PA.



Acme Ltd.

Legal,Leisure,Pharmaceuticals,Transport
Other
Small (<50 employees, ≤€10M turnover)

5
Processing activities

Profile completeness 100%

Basic Data | Contacts | Generic asset profile | Assets inventory

Assets inventory
4 of 5 assets

+ Add

Asset	Related PA(s)	Vendor	Product	CPE/version	Criticality	Rel.assets	Rel.OTMs	Actions
Acme Website CMS The public website of the company Sales via DrupalCommerce	**Marketing Fulfill customer order**	drupal	drupal	8.9.2	-	-	-	
Xerox WorkCentre 7970i Cloud printer for processing payroll	**-**	xerox	xeroxworkcentre_7970i	5.3.1	High	-	-	
Microsoft Office 365 Office suite used by HR dept	**Payroll Processing**	microsoft	365_apps	7.3.1	Low	-	-	
Brightpay Cloud A Cloud sodtware suite for payroll processing	**Payroll Processing**	brightpay	Brightpay Cloud	9.0.1	Low	-	-	

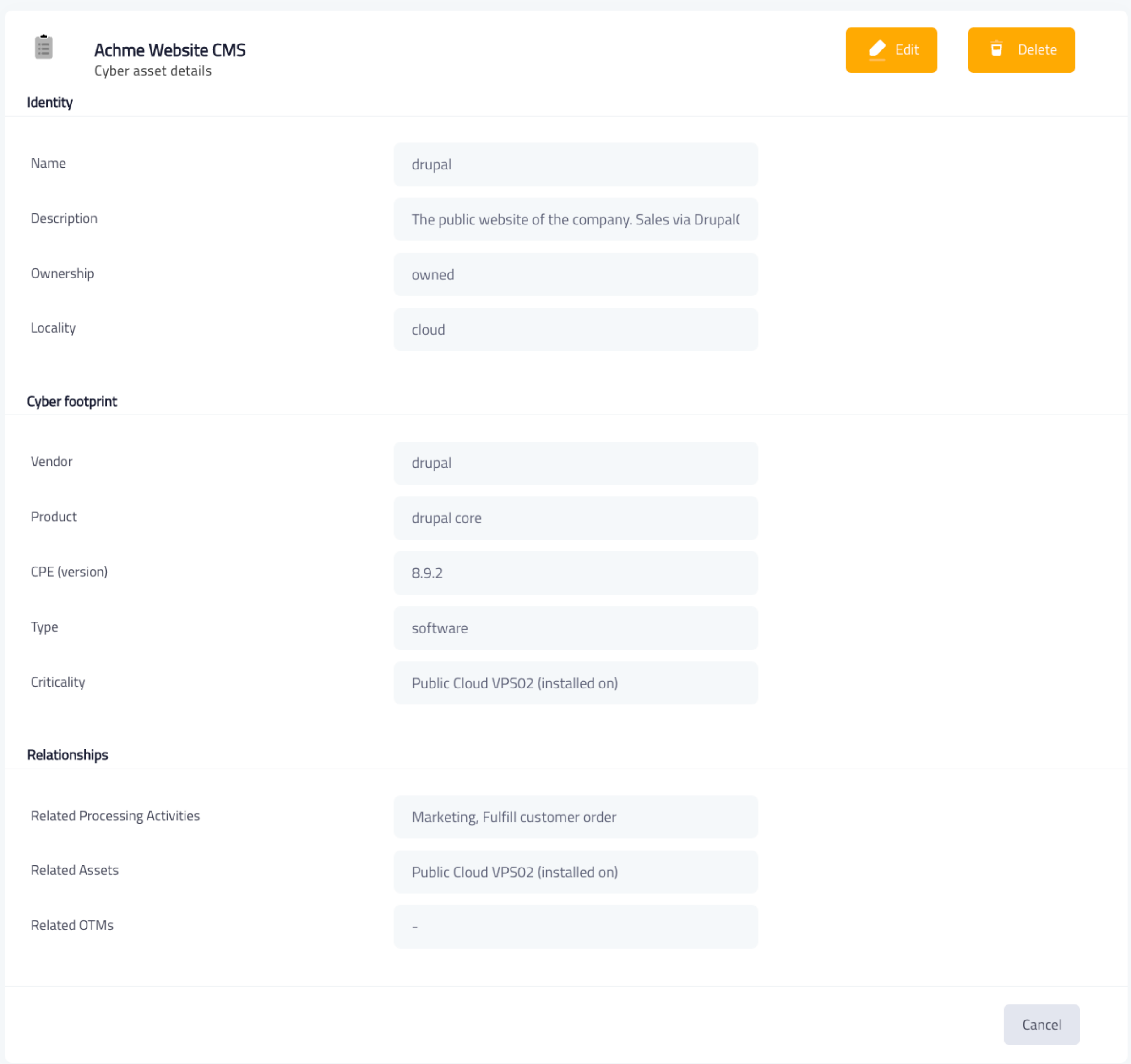
Items per page: 5 | 1 – 2 of 2

Figure 18. "Asset inventory" tab of the My Organization menu item

It includes:

- Asset: The name of the asset and a short description.
- Related PA(s): Which PAs are related to the specific asset.
- Vendor: The vendor of the asset.
- Product: The specific product related to the asset.
- CPE/Version: The version of the product.
- Criticality: The criticality associated with the asset.
- Related assets: Assets related to the specific asset.
- Related OTMs: OTMs related to the specific asset.
- Actions: View/Edit/Delete the asset from the organizational profile.

By clicking the "View" button (magnifying glass on the right-hand side) of a specific asset, the user is redirected to the corresponding page, where they can see in an extended manner all the information pertaining to the specific asset, as described above (Figure 19).



Achme Website CMS
Cyber asset details

Identity

Name	drupal
Description	The public website of the company. Sales via Drupal(
Ownership	owned
Locality	cloud

Cyber footprint

Vendor	drupal
Product	drupal core
CPE (version)	8.9.2
Type	software
Criticality	Public Cloud VPS02 (installed on)

Relationships

Related Processing Activities	Marketing, Fulfill customer order
Related Assets	Public Cloud VPS02 (installed on)
Related OTMs	-

Figure 19. Details of a specific asset

If the user wishes to edit the specific asset, they can do so by clicking on the "Edit" button on the top right. Then, all the page fields become writable and the user can input their data. The "Delete" button deletes the specific asset.

4.4 Data protection

This is a dropdown menu item. By clicking on it, the user is presented with the corresponding links "Processing Activities" and "ROPA" (Figure 20). The "ROPA" link is a new addition to the platform. More links and content will be added in future versions.

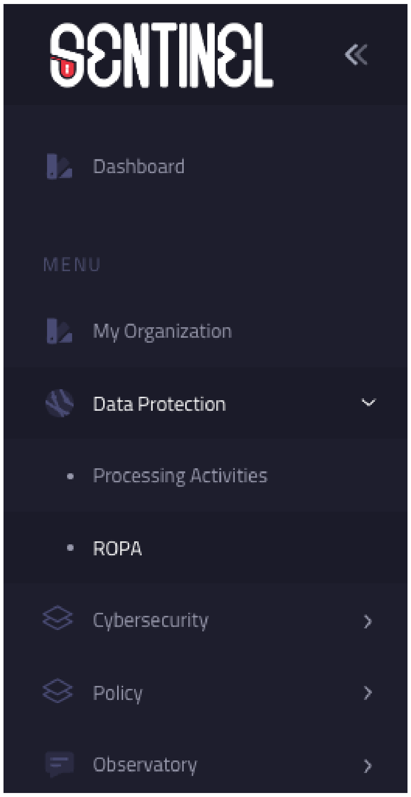


Figure 20. Data Protection dropdown menu

4.4.1 Processing Activities

The "Processing Activities" link directs the user to the Processing Activities overview page where they can view the relevant PAs stored in the system and perform some kind of action on them (View/Edit/Delete).

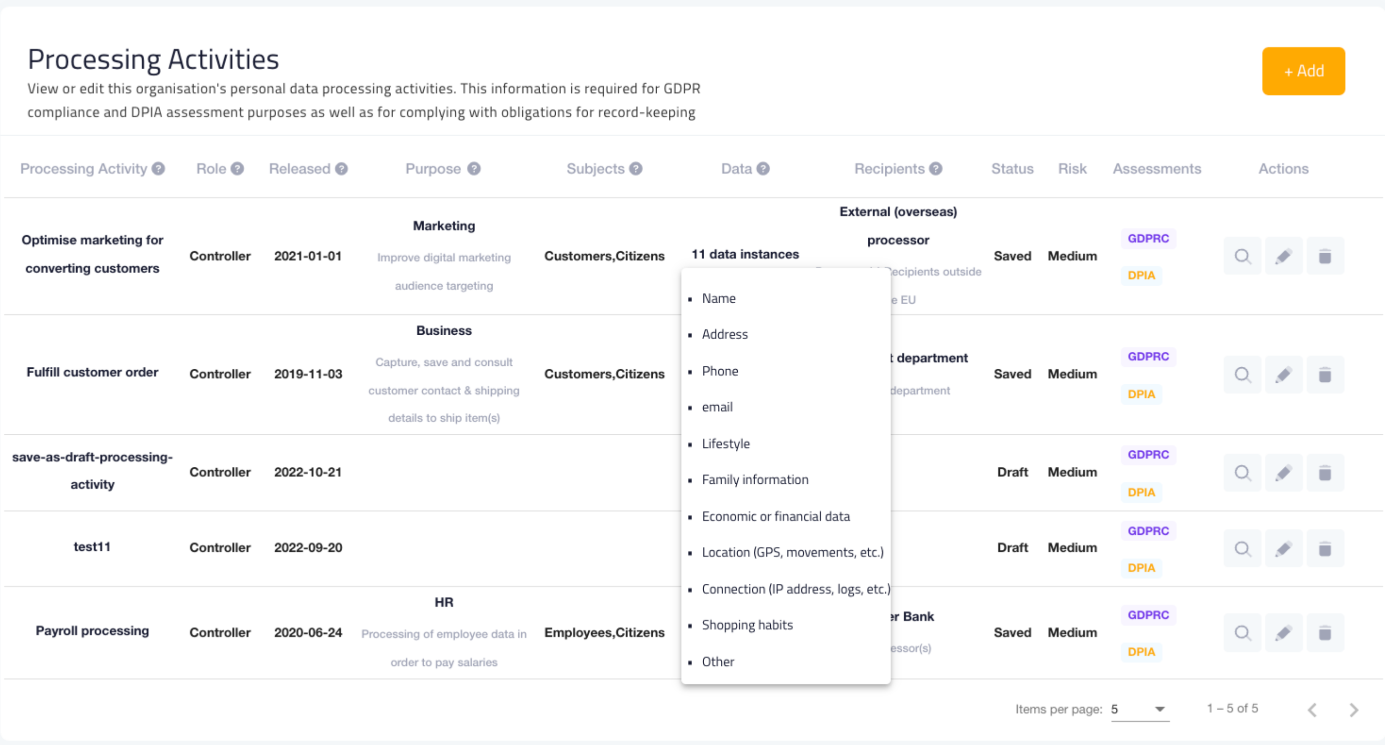
Processing Activities overview

This page (Figure 21) contains a table with all the personal data PAs that are associated with the specific organization. A number of UI updates have been carried out since the MVP version for better user experience (font, colours, tables, drop-down menus, etc.), most notable of which is the "Data" categories column, where the categories are displayed in a list for better visibility.

As depicted, the columns of the table are:

- Processing Activity: A short name to identify the specific personal data PA. It is clickable and leads to specific PA's page.
- Role: The GDPR role of the organisation regarding the data processed in the PA. Either "Controller" (owner – responsible for all collection and processing of personal data), or "Processor" (possibly third-party – responsible for limited processing of personal data)
- Released: The date when the PA was first released to the public.

- Purpose: Category for processing (in bold). Why the data need to be processed (as a subtitle).
- Subjects: Natural persons subject to personal data processing in the PA.
- Data: The type of data being processed.
- Recipients: Recipients of the data in the PA.
- Status: The status of the PA (Complete or Draft).
- Risk: The risk associated with a specific PA.
- Assessments: Buttons to perform GDPR Compliance Assessment (GDPRC) or Data Protection Impact Assessment (DPIA). They are active only if the corresponding assessments are available, depending on the status of the PA, which needs to be Complete.
- Actions: Buttons that the user can click, to perform additional actions, i.e., “View” (the Magnifying Glass icon – can also be performed by clicking on the PA’s name), “Edit” (the Pencil icon) and “Delete” (the Rubbish Bin icon).



Processing Activities

View or edit this organisation's personal data processing activities. This information is required for GDPR compliance and DPIA assessment purposes as well as for complying with obligations for record-keeping

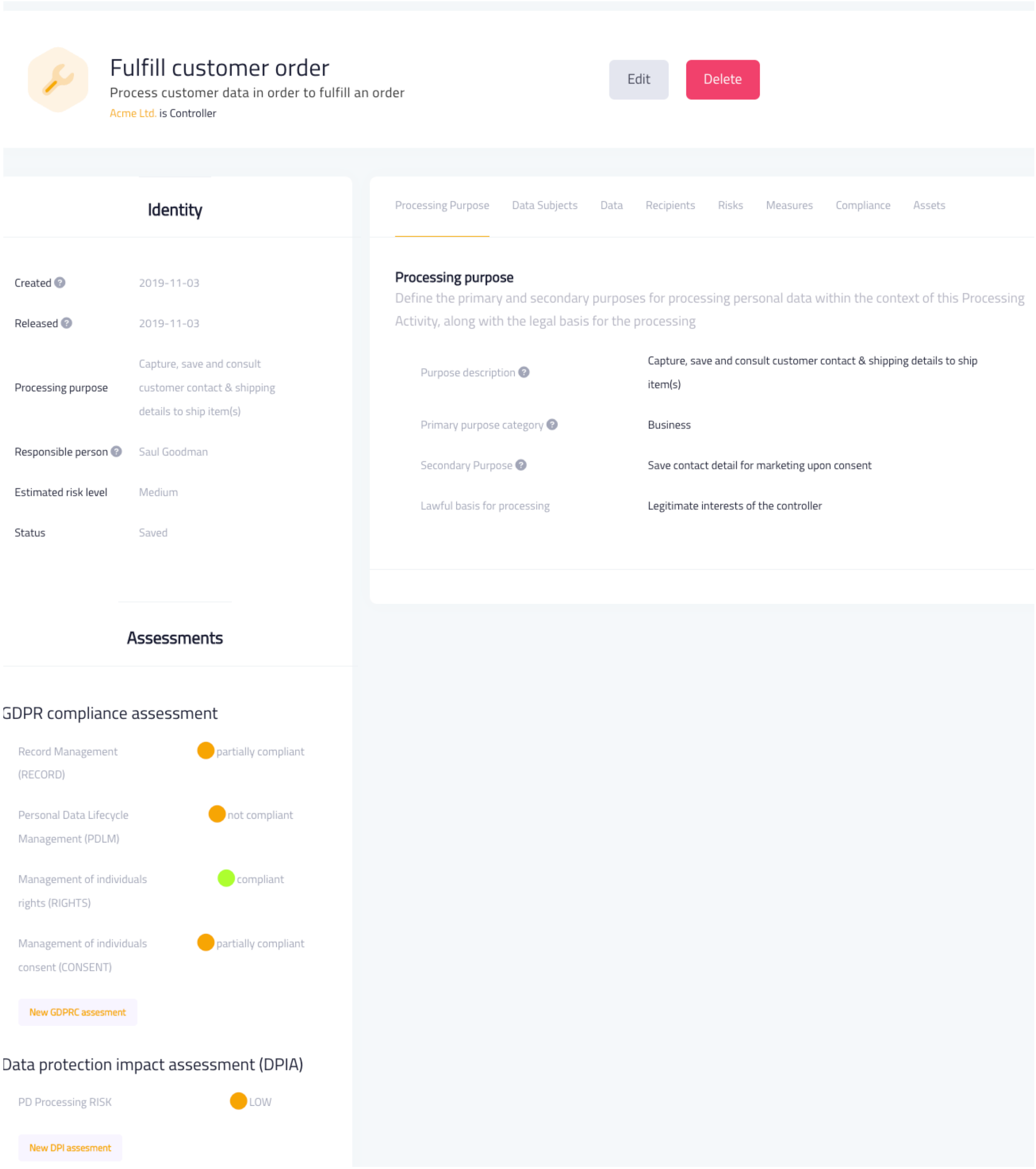
Processing Activity ?	Role ?	Released ?	Purpose ?	Subjects ?	Data ?	Recipients ?	Status	Risk	Assessments	Actions
Optimise marketing for converting customers	Controller	2021-01-01	**Marketing** Improve digital marketing audience targeting	Customers,Citizens	11 data instances ▪ Name ▪ Address ▪ Phone ▪ email ▪ Lifestyle ▪ Family information ▪ Economic or financial data ▪ Location (GPS, movements, etc.) ▪ Connection (IP address, logs, etc.) ▪ Shopping habits ▪ Other	**External (overseas) processor** ecipients outside e EU	Saved	Medium	GDPRC DPIA	🔍 ✎ 🗑
Fulfill customer order	Controller	2019-11-03	**Business** Capture, save and consult customer contact & shipping details to ship item(s)	Customers,Citizens		**t department** department	Saved	Medium	GDPRC DPIA	🔍 ✎ 🗑
save-as-draft-processing-activity	Controller	2022-10-21					Draft	Medium	GDPRC DPIA	🔍 ✎ 🗑
test11	Controller	2022-09-20					Draft	Medium	GDPRC DPIA	🔍 ✎ 🗑
Payroll processing	Controller	2020-06-24	**HR** Processing of employee data in order to pay salaries	Employees,Citizens		**r Bank** essor(s)	Saved	Medium	GDPRC DPIA	🔍 ✎ 🗑

Items per page: 5 1 – 5 of 5

Figure 21. PA updates

View individual Processing Activity

Upon clicking either the name of a PA or the respective “View” button, the user is redirected to the individual page of the specific PA. There, they can see the details of the PA, as shown in Figure 22.



Fulfill customer order

Process customer data in order to fulfill an order

Acme Ltd. is Controller

Identity

Created	2019-11-03
Released	2019-11-03
Processing purpose	Capture, save and consult customer contact & shipping details to ship item(s)
Responsible person	Saul Goodman
Estimated risk level	Medium
Status	Saved

Assessments

GDPR compliance assessment

Record Management (RECORD)	● partially compliant
Personal Data Lifecycle Management (PDLM)	● not compliant
Management of individuals rights (RIGHTS)	● compliant
Management of individuals consent (CONSENT)	● partially compliant

Data protection impact assessment (DPIA)

PD Processing RISK	● LOW

Processing purpose

Define the primary and secondary purposes for processing personal data within the context of this Processing Activity, along with the legal basis for the processing

Purpose description	Capture, save and consult customer contact & shipping details to ship item(s)
Primary purpose category	Business
Secondary Purpose	Save contact detail for marketing upon consent
Lawful basis for processing	Legitimate interests of the controller

Figure 22. Individual Processing Activity view page

The name of the PA is visible at the top of the page. Under it there are the GDPR roles of the organisation, as described in the previous paragraph. On the right, the user may find buttons in order to “Edit” or “Delete” the PA.

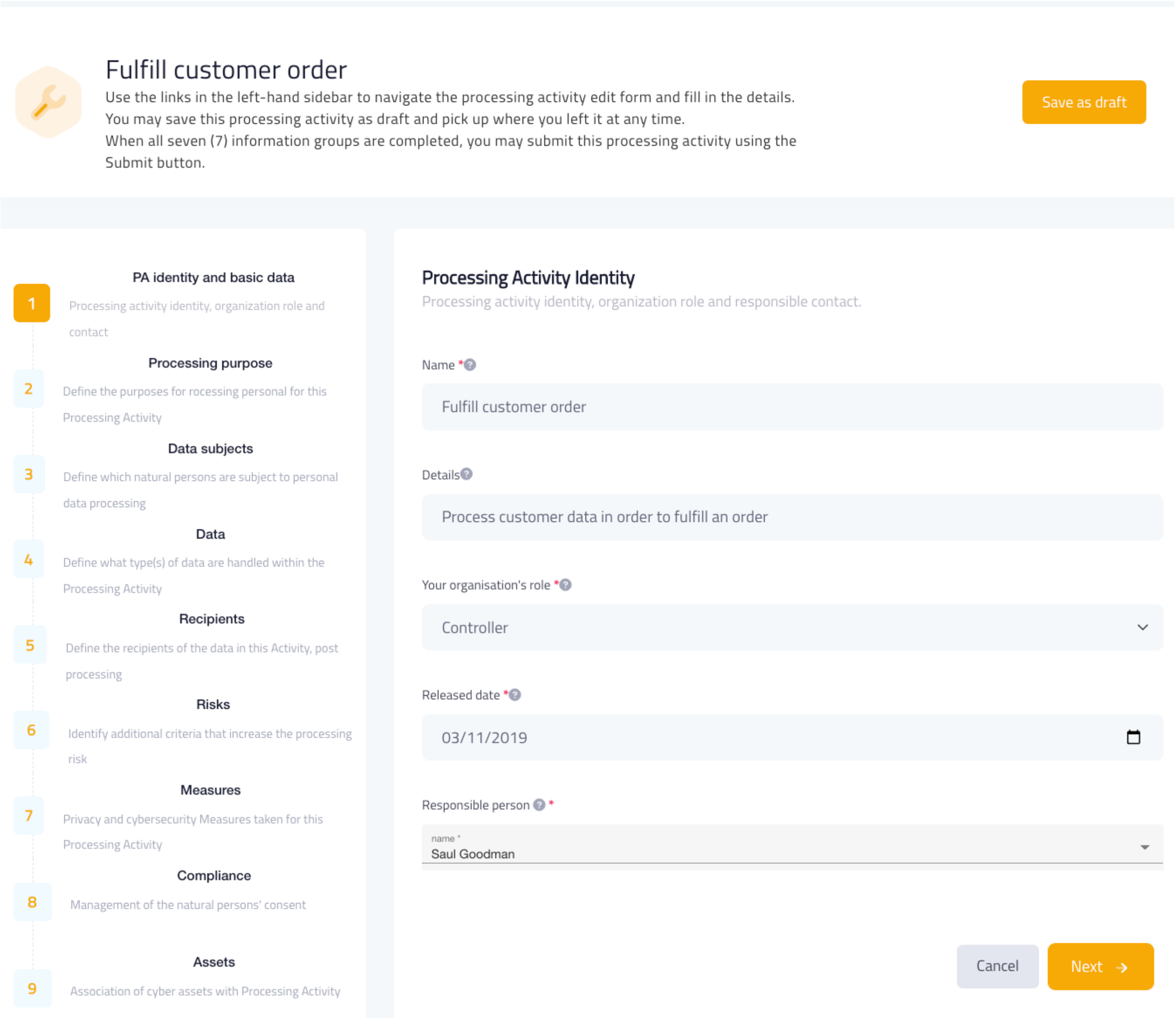
In the left section, the user can see the identity of the PA (as described in the previous paragraph) and information on the Assessments. If one has not been performed, the relevant button appears to indicate that the user can do the associated assessment.

On the right section, there are several tabs with information associated with the PA (these are summarized in the overview page, as described in Figure 21):

- Processing purpose: The primary and secondary purposes for processing personal data within the context of the PA, along with the legal basis for the processing.
- Data subjects: The natural persons subject to personal data processing in the PA and vulnerable or sensitive subjects that may have been identified.
- Data: Type(s) of data that are handled within the context of the PA and sensitive data that may have been identified.
- Recipients: The recipients of the data in the PA, post-processing
- Risks: Additional criteria that increase the processing risk for subjects/individuals, if any.
- Measures: Organizational and technical measures taken to increase the privacy and cybersecurity of the PA, for the protection of personal data.
- Compliance: Content in this tab will be added in future versions.
- Assets: The assets that are linked to the specific PA.

Create new / Edit specific Processing Activity

The pages above also contain “Add” and “Edit” buttons that create a new or update an existing PA. When doing so, the user navigates to the page shown in Figure 23.



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

1 PA identity and basic data
Processing activity identity, organization role and contact

2 Processing purpose
Define the purposes for rocessing personal for this Processing Activity

3 Data subjects
Define which natural persons are subject to personal data processing

4 Data
Define what type(s) of data are handled within the Processing Activity

5 Recipients
Define the recipients of the data in this Activity, post processing

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

8 Compliance
Management of the natural persons' consent

9 Assets
Association of cyber assets with Processing Activity

Processing Activity Identity

Processing activity identity, organization role and responsible contact.

Name *: Fulfill customer order

Details: Process customer data in order to fulfill an order

Your organisation's role *: Controller

Released date *: 03/11/2019

Responsible person *: name * Saul Goodman

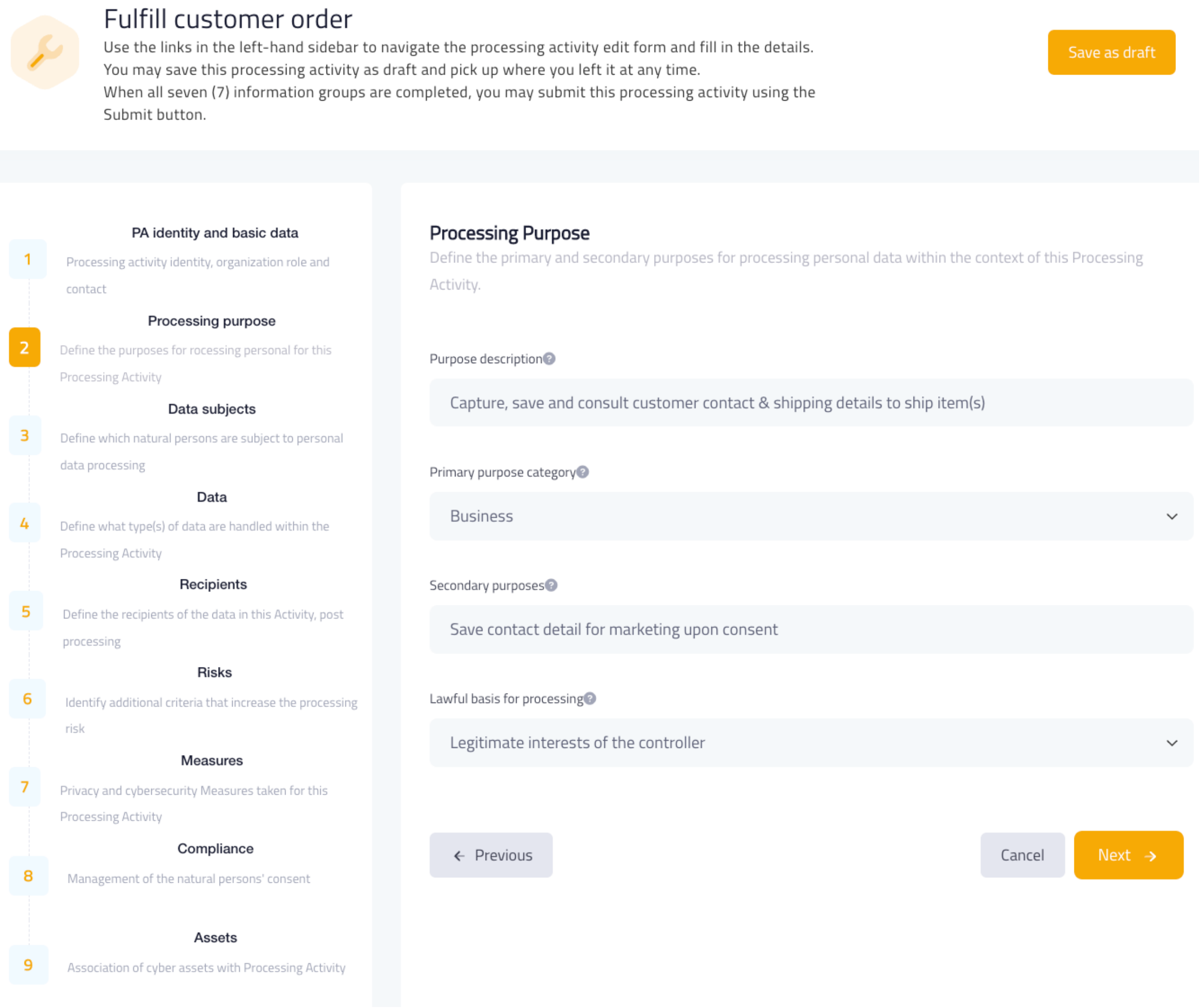
Figure 23. Create new / Edit specific Processing Activity page

This is a form that has nine stages, where the user can fill in all the relevant information and save their progress. These are the data shown in the pages described in the previous paragraphs.

As depicted in Figures Figure 23 – Figure 31, the user must fill in:

- The PA's identity, organization role, processor, release date and responsible contact (Figure 23).
- The primary and secondary purposes for processing personal data within the context of the PA (Figure 24).

- The natural persons subject to personal data processing in the PA and identify vulnerable or sensitive subjects (Figure 25).
- The type(s) of data that are handled within the context of the PA and identify sensitive data (Figure 26).
- The recipients of the data in the PA, post-processing (Figure 27).
- Additional criteria that increase the processing risk for subjects/individuals, if any (Figure 28).
- Organizational and technical measures taken to increase the privacy and cybersecurity of the PA, for the protection of personal data (Figure 29 – screenshot not complete for the sake of visibility).



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

1 PA identity and basic data — Processing activity identity, organization role and contact

2 Processing purpose — Define the purposes for rocessing personal for this Processing Activity

3 Data subjects — Define which natural persons are subject to personal data processing

4 Data — Define what type(s) of data are handled within the Processing Activity

5 Recipients — Define the recipients of the data in this Activity, post processing

6 Risks — Identify additional criteria that increase the processing risk

7 Measures — Privacy and cybersecurity Measures taken for this Processing Activity

8 Compliance — Management of the natural persons' consent

9 Assets — Association of cyber assets with Processing Activity

Processing Purpose

Define the primary and secondary purposes for processing personal data within the context of this Processing Activity.

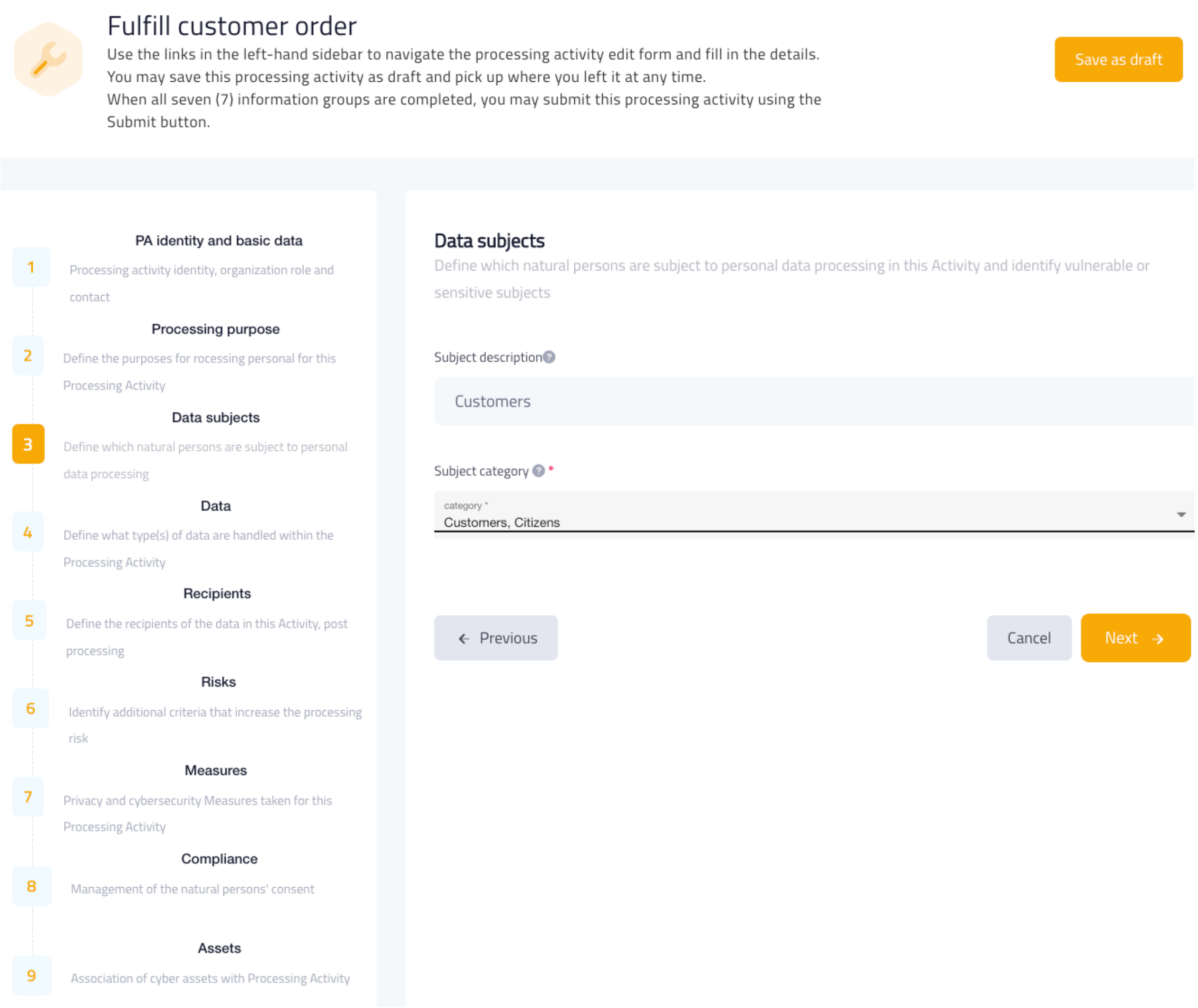
Purpose description: Capture, save and consult customer contact & shipping details to ship item(s)

Primary purpose category: Business

Secondary purposes: Save contact detail for marketing upon consent

Lawful basis for processing: Legitimate interests of the controller

Figure 24. Provide input for the Processing Purpose of the PA



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

1 **PA identity and basic data**
Processing activity identity, organization role and contact

2 **Processing purpose**
Define the purposes for rocessing personal for this Processing Activity

3 **Data subjects**
Define which natural persons are subject to personal data processing

4 **Data**
Define what type(s) of data are handled within the Processing Activity

5 **Recipients**
Define the recipients of the data in this Activity, post processing

6 **Risks**
Identify additional criteria that increase the processing risk

7 **Measures**
Privacy and cybersecurity Measures taken for this Processing Activity

8 **Compliance**
Management of the natural persons' consent

9 **Assets**
Association of cyber assets with Processing Activity

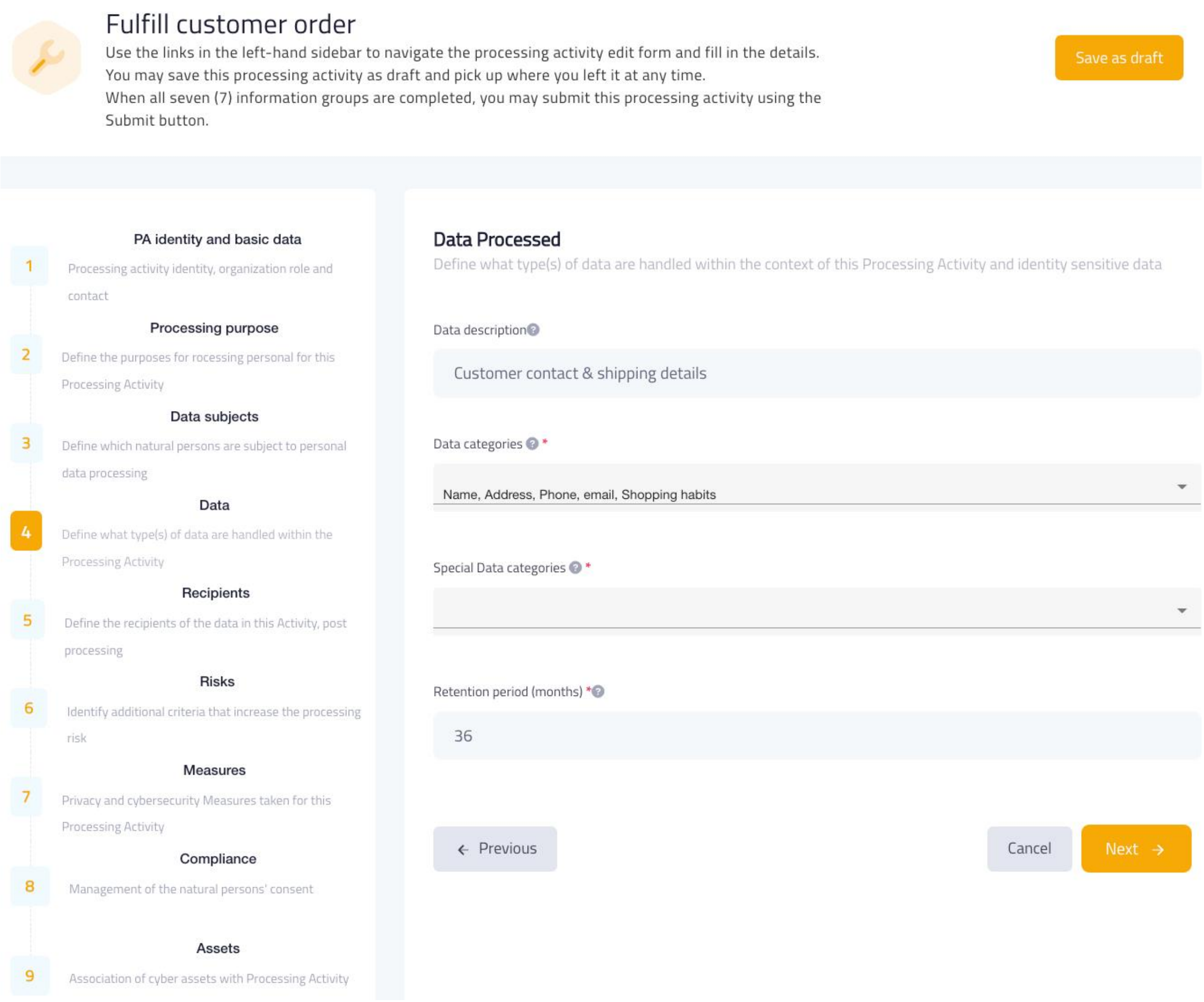
Data subjects

Define which natural persons are subject to personal data processing in this Activity and identify vulnerable or sensitive subjects

Subject description
Customers

Subject category *
category *
Customers, Citizens

Figure 25. Provide input for the Data Subjects of the PA



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

1 PA identity and basic data
Processing activity identity, organization role and contact

2 Processing purpose
Define the purposes for rocessing personal for this Processing Activity

3 Data subjects
Define which natural persons are subject to personal data processing

4 Data
Define what type(s) of data are handled within the Processing Activity

5 Recipients
Define the recipients of the data in this Activity, post processing

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

8 Compliance
Management of the natural persons' consent

9 Assets
Association of cyber assets with Processing Activity

Data Processed

Define what type(s) of data are handled within the context of this Processing Activity and identity sensitive data

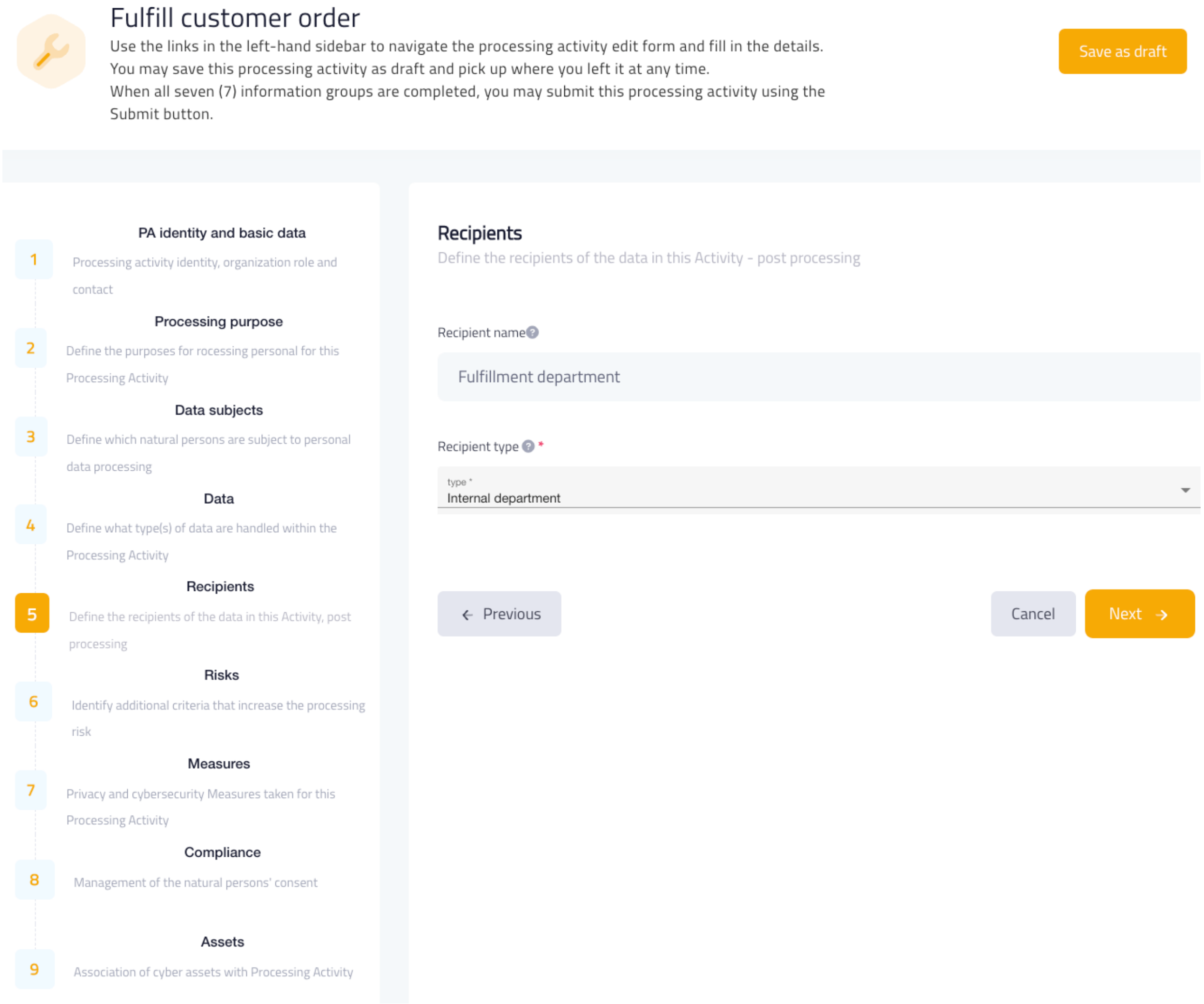
Data description: Customer contact & shipping details

Data categories *: Name, Address, Phone, email, Shopping habits

Special Data categories *:

Retention period (months) *: 36

Figure 26. Provide input for the Data of the PA



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

1 PA identity and basic data
Processing activity identity, organization role and contact

2 Processing purpose
Define the purposes for rocessing personal for this Processing Activity

3 Data subjects
Define which natural persons are subject to personal data processing

4 Data
Define what type(s) of data are handled within the Processing Activity

5 Recipients
Define the recipients of the data in this Activity, post processing

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

8 Compliance
Management of the natural persons' consent

9 Assets
Association of cyber assets with Processing Activity

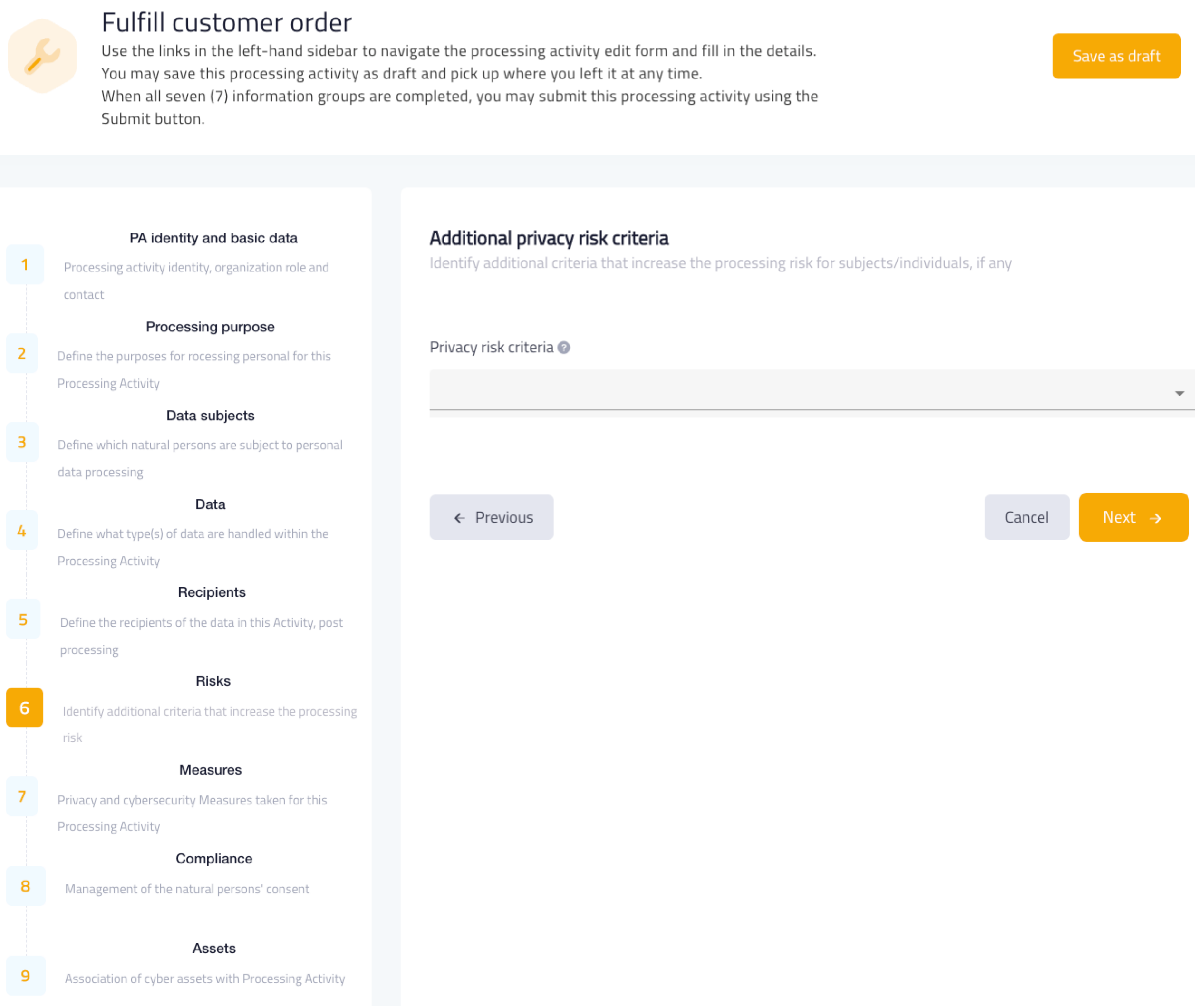
Recipients

Define the recipients of the data in this Activity - post processing

Recipient name: Fulfillment department

Recipient type *: type * Internal department

Figure 27. Provide input for the Recipients of the PA



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

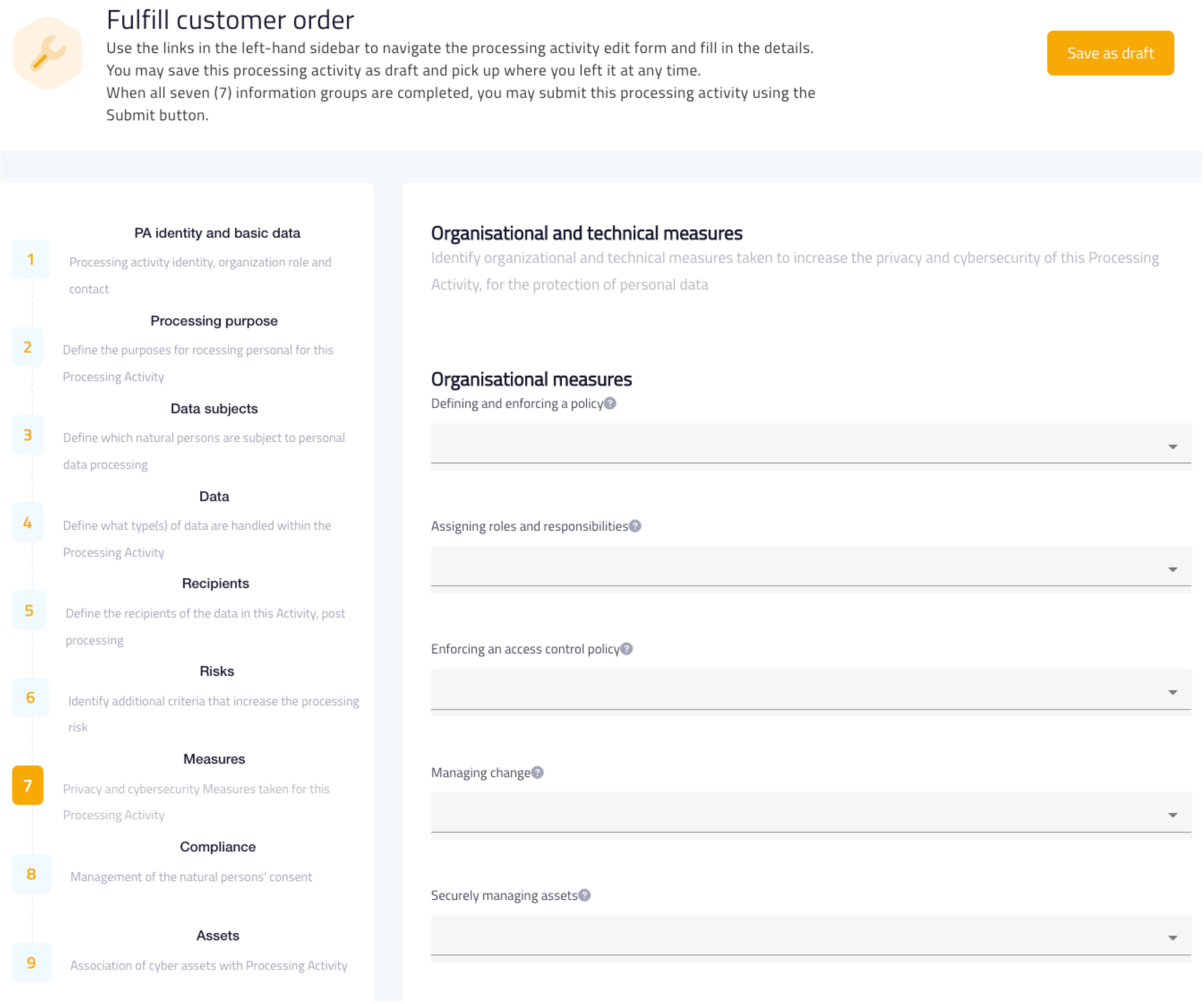
1 PA identity and basic data
Processing activity identity, organization role and contact
2 Processing purpose
Define the purposes for rocessing personal for this Processing Activity
3 Data subjects
Define which natural persons are subject to personal data processing
4 Data
Define what type(s) of data are handled within the Processing Activity
5 Recipients
Define the recipients of the data in this Activity, post processing
6 Risks
Identify additional criteria that increase the processing risk
7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity
8 Compliance
Management of the natural persons' consent
9 Assets
Association of cyber assets with Processing Activity

Additional privacy risk criteria

Identify additional criteria that increase the processing risk for subjects/individuals, if any

Privacy risk criteria

Figure 28. Provide input for the Risks of the PA



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

1 PA identity and basic data
Processing activity identity, organization role and contact

2 Processing purpose
Define the purposes for rocessing personal for this Processing Activity

3 Data subjects
Define which natural persons are subject to personal data processing

4 Data
Define what type(s) of data are handled within the Processing Activity

5 Recipients
Define the recipients of the data in this Activity, post processing

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

8 Compliance
Management of the natural persons' consent

9 Assets
Association of cyber assets with Processing Activity

Organisational and technical measures

Identify organizational and technical measures taken to increase the privacy and cybersecurity of this Processing Activity, for the protection of personal data

Organisational measures

Defining and enforcing a policy

Assigning roles and responsibilities

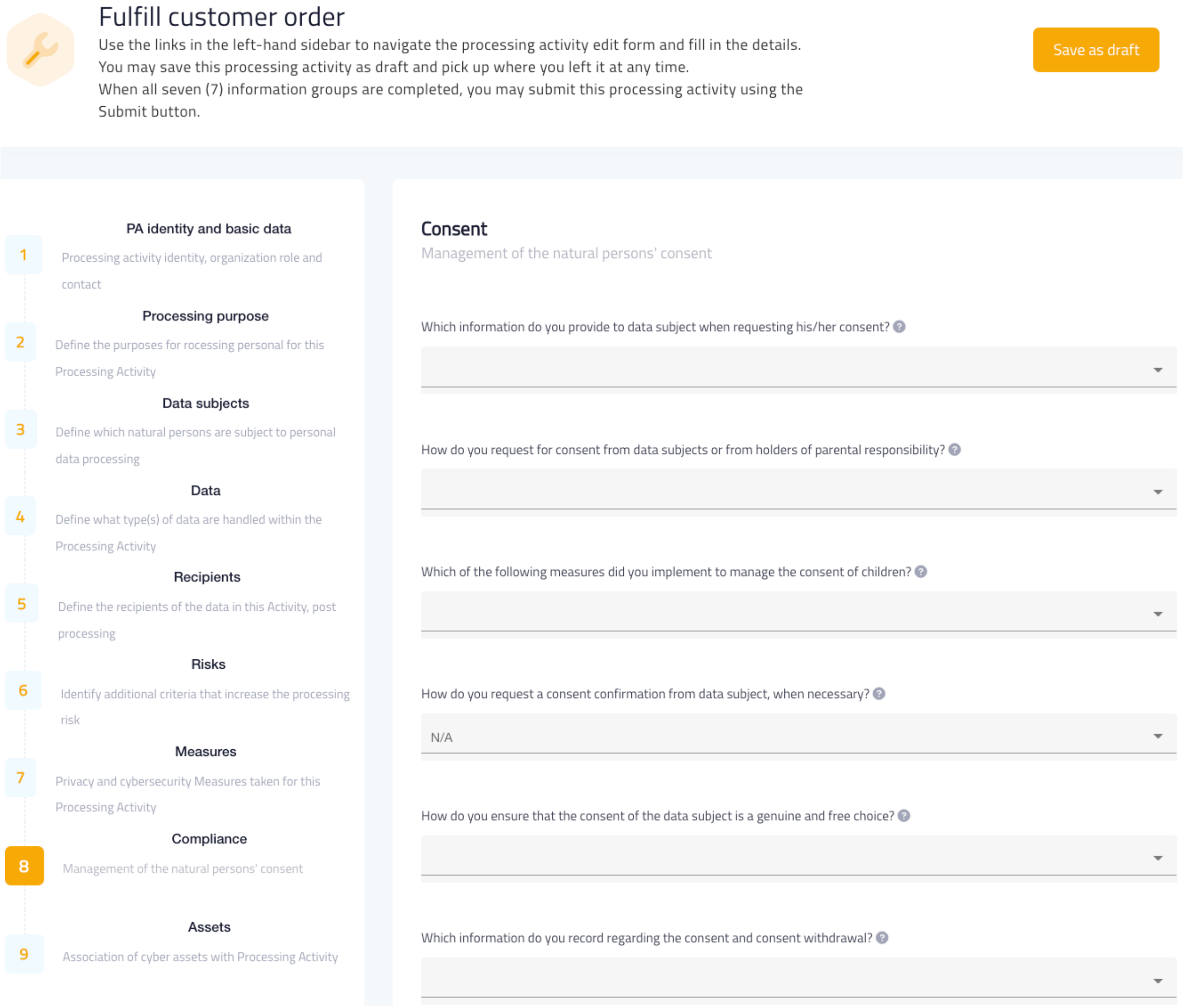
Enforcing an access control policy

Managing change

Securely managing assets

Figure 29. Provide input for the Measures of the PA

In addition to the pages above that are included in the MVP version of the platform, in this version we add two more steps in the corresponding wizard (“Compliance” and “Assets”). In the “Compliance” step (Figure 30), the SME representative is asked to give input about how their organization manages a person’s consent.



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

1 PA identity and basic data
Processing activity identity, organization role and contact

2 Processing purpose
Define the purposes for rocessing personal for this Processing Activity

3 Data subjects
Define which natural persons are subject to personal data processing

4 Data
Define what type(s) of data are handled within the Processing Activity

5 Recipients
Define the recipients of the data in this Activity, post processing

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

8 Compliance
Management of the natural persons' consent

9 Assets
Association of cyber assets with Processing Activity

Consent
Management of the natural persons' consent

Which information do you provide to data subject when requesting his/her consent?

How do you request for consent from data subjects or from holders of parental responsibility?

Which of the following measures did you implement to manage the consent of children?

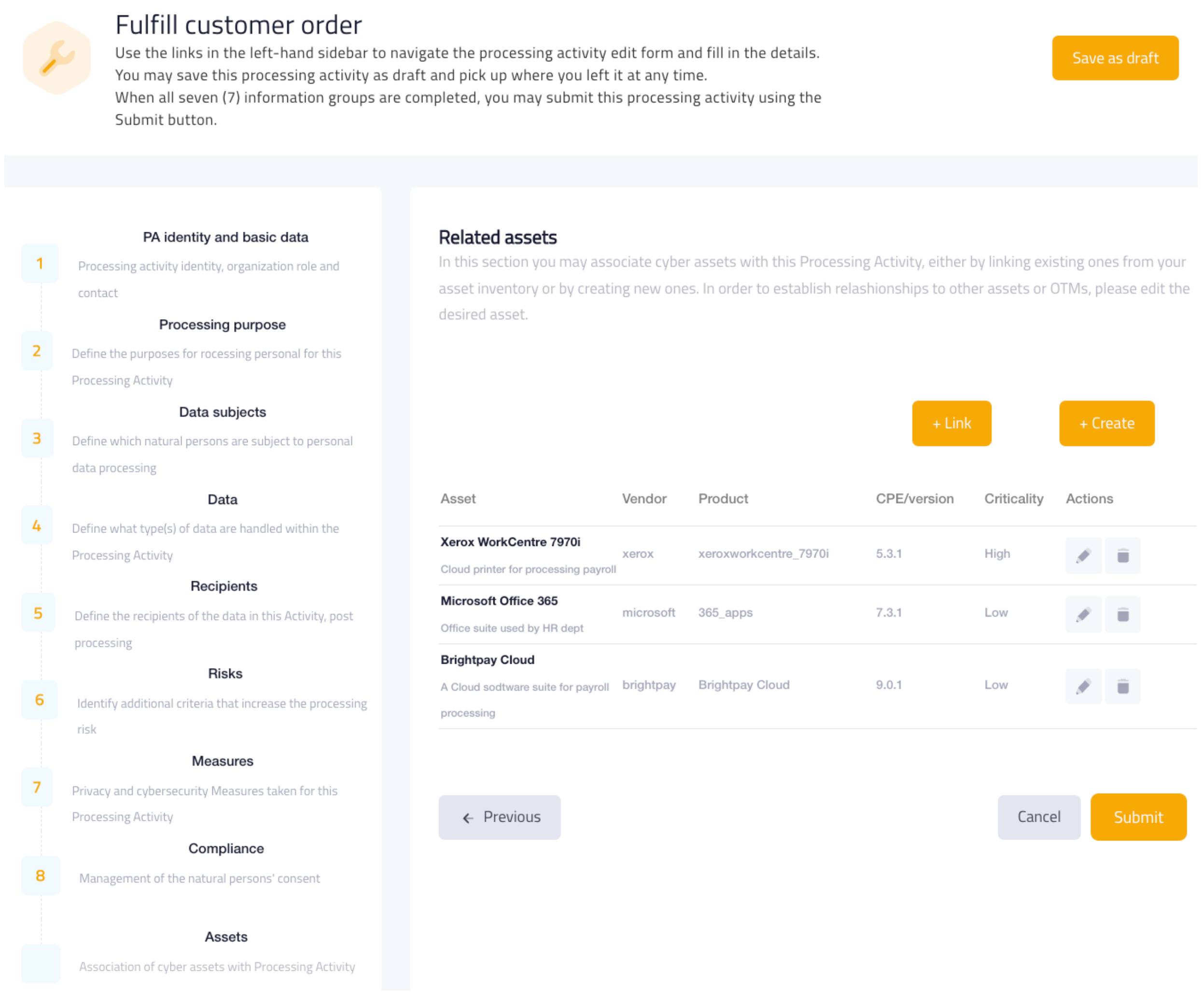
How do you request a consent confirmation from data subject, when necessary?
N/A

How do you ensure that the consent of the data subject is a genuine and free choice?

Which information do you record regarding the consent and consent withdrawal?

Figure 30. Provide input for the Management of a natural person's consent

In Figure 31, the asset capturing page can be seen, where the user can create a new asset and link in with the specific PA.



Fulfill customer order

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 seven (7) information groups are completed, you may submit this processing activity using the Submit button.

1 PA identity and basic data
Processing activity identity, organization role and contact

2 Processing purpose
Define the purposes for rocessing personal for this Processing Activity

3 Data subjects
Define which natural persons are subject to personal data processing

4 Data
Define what type(s) of data are handled within the Processing Activity

5 Recipients
Define the recipients of the data in this Activity, post processing

6 Risks
Identify additional criteria that increase the processing risk

7 Measures
Privacy and cybersecurity Measures taken for this Processing Activity

8 Compliance
Management of the natural persons' consent

Assets
Association of cyber assets with Processing Activity

Related assets

In this section you may associate cyber assets with this Processing Activity, either by linking existing ones from your asset inventory or by creating new ones. In order to establish relashionships to other assets or OTMs, please edit the desired asset.

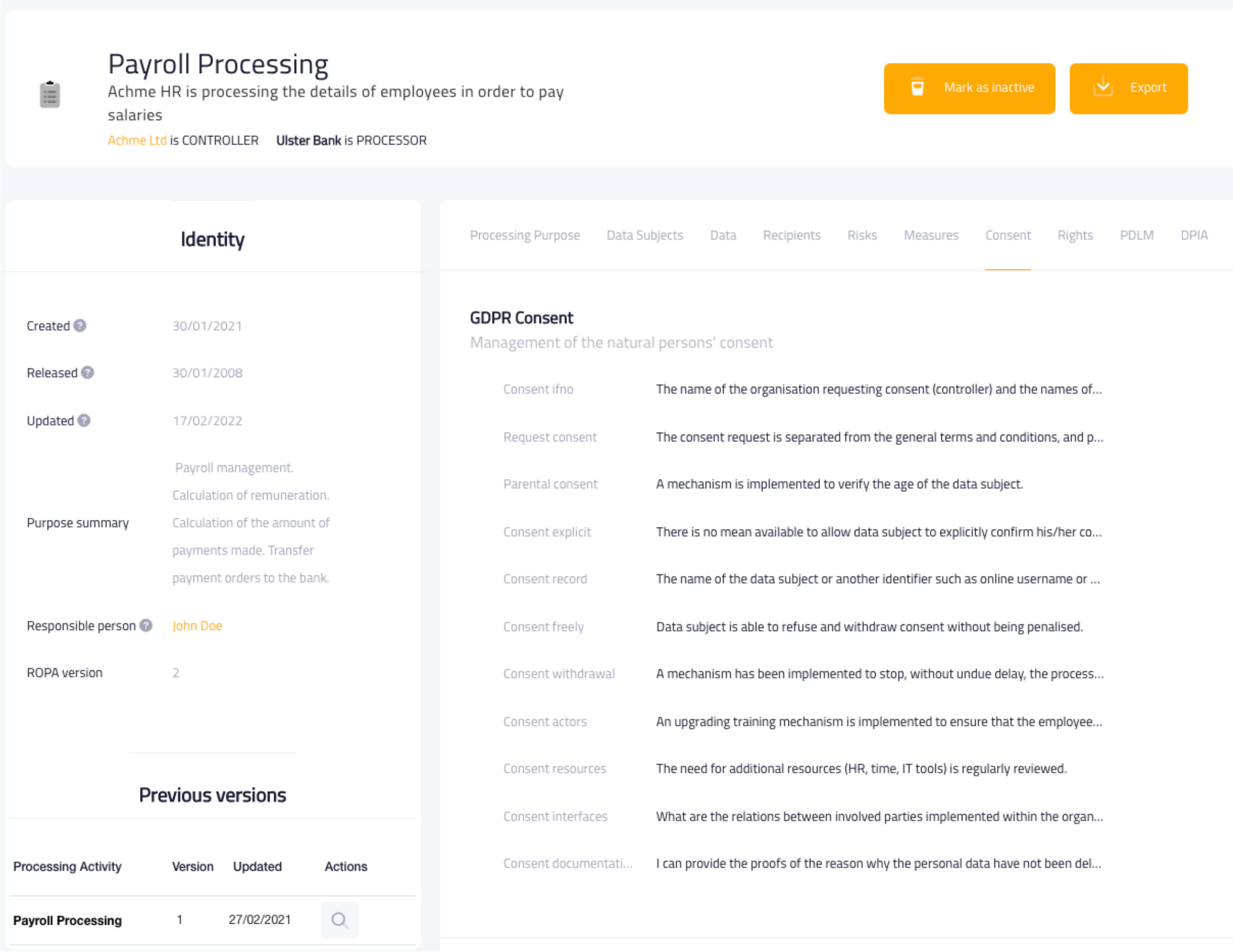
Asset	Vendor	Product	CPE/version	Criticality	Actions
Xerox WorkCentre 7970i Cloud printer for processing payroll	xerox	xeroxworkcentre_7970i	5.3.1	High	
Microsoft Office 365 Office suite used by HR dept	microsoft	365_apps	7.3.1	Low	
Brightpay Cloud A Cloud sodtware suite for payroll processing	brightpay	Brightpay Cloud	9.0.1	Low	

Figure 31. Asset capturing when creating/editing a PA

When the user is ready, they can go to the “Next” stage or move to the “Previous” one. They can, also, “Cancel” the procedure whenever they choose, thus returning to the PA overview page (Figure 21). Upon filling in all the fields in all the stages of the form (and only then), the user can “Submit” the PA to the platform’s database. All these buttons are found at the bottom of the page. At any point in the process, the user is able to “Save as draft” the PA with their progress so far (top right of the page), in order to return later and finish creating the PA. Similarly, when editing an existing/draft PA, all the form fields are pre-filled with their respective values (where applicable) and cancelling the process returns the user to the individual PA view page (Figure 23).

4.4.2 Record of Processing Activity (ROPA)

This menu item link is a new addition to the platform. It leads the user to the record of a specific PA where they can view the relevant information stored in the system (Figure 32).



Payroll Processing

Achme HR is processing the details of employees in order to pay salaries

Achme Ltd is CONTROLLER Ulster Bank is PROCESSOR

Identity

Created	30/01/2021
Released	30/01/2008
Updated	17/02/2022
Purpose summary	Payroll management. Calculation of remuneration. Calculation of the amount of payments made. Transfer payment orders to the bank.
Responsible person	John Doe
ROPA version	2

Previous versions

Processing Activity	Version	Updated	Actions
Payroll Processing	1	27/02/2021	

GDPR Consent

Management of the natural persons' consent

Consent ifno	The name of the organisation requesting consent (controller) and the names of...
Request consent	The consent request is separated from the general terms and conditions, and p...
Parental consent	A mechanism is implemented to verify the age of the data subject.
Consent explicit	There is no mean available to allow data subject to explicitly confirm his/her co...
Consent record	The name of the data subject or another identifier such as online username or ...
Consent freely	Data subject is able to refuse and withdraw consent without being penalised.
Consent withdrawal	A mechanism has been implemented to stop, without undue delay, the process...
Consent actors	An upgrading training mechanism is implemented to ensure that the employee...
Consent resources	The need for additional resources (HR, time, IT tools) is regularly reviewed.
Consent interfaces	What are the relations between involved parties implemented within the organ...
Consent documentati...	I can provide the proofs of the reason why the personal data have not been del...

Figure 32. ROPA of a specific PA

At the left-hand side of the page, there is information about the identity of the PA and below it the user can see any previous versions that the specific PA may have (e.g. after updating it). On the right-hand side there is more detailed information about the specific PA:

- Processing Purpose: Category for processing. Why the data need to be processed.
- Data subjects: Natural persons subject to personal data processing in the PA.
- Data: The type of data being processed.
- Recipients: Recipients of the data in the PA.
- Risks: The risks associated with the specific PA.
- Measures: Operational and Technical Measures (OTMs) associated with the specific PA.
- Assets: The organization’s cyber assets associated with the specific PA.
- Consent: Questions related to GDPR and management of the natural persons' consent
- Rights: Questions related to GDPR and management of the natural persons' rights
- PDLM: Questions related to GDPR and Personal Data Lifecycle Management
- DPIA: The Data Protection Impact Assessment performed for the PA

All this information is provided by the user at the creation/editing stage of the PA and after saving the PA to the ROPA, it is displayed here.

4.5 Cybersecurity

This is another dropdown menu item, similar to "Data Protection". By clicking on it, the user is presented with the corresponding links "Assets", "Measures", "Simulation Environment", "Cyber Range" and "FVT" (Figure 33). Assets, Measures and FVT are new additions to the platform. More links and content will be added in future versions.

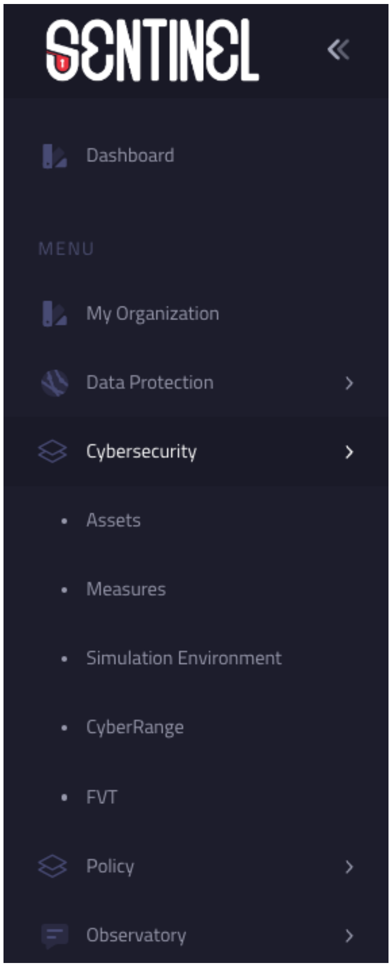
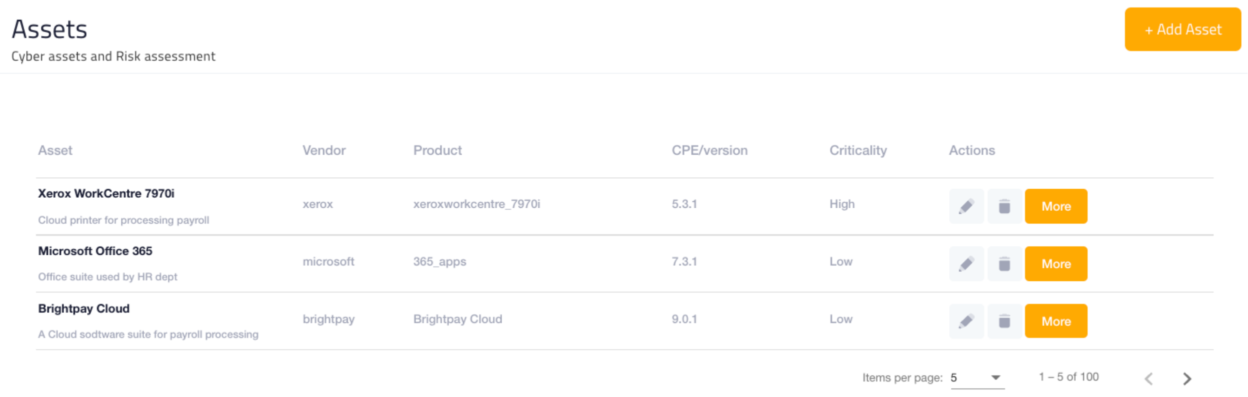


Figure 33. Cybersecurity dropdown menu

4.5.1 Assets

By visiting the "Assets" page, the user has the opportunity to see a listing with all the assets of their organization. The columns (Asset, Vendor, Product, CPE/version, Criticality, Actions) are similar to the ones explained in Section 4.3.4 (Figure 34).



Assets

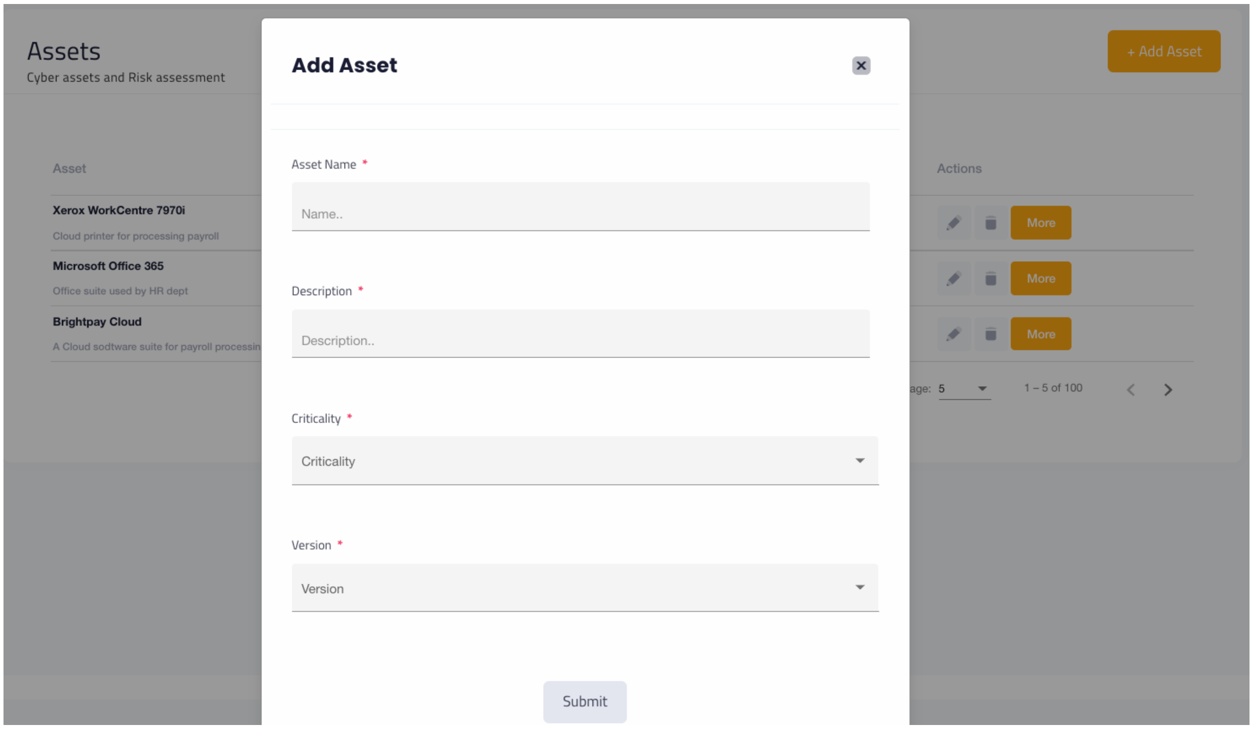
Cyber assets and Risk assessment

Asset	Vendor	Product	CPE/version	Criticality	Actions
Xerox WorkCentre 7970i Cloud printer for processing payroll	xerox	xeroxworkcentre_7970i	5.3.1	High	More
Microsoft Office 365 Office suite used by HR dept	microsoft	365_apps	7.3.1	Low	More
Brightpay Cloud A Cloud sodtware suite for payroll processing	brightpay	Brightpay Cloud	9.0.1	Low	More

Items per page: 5 1 – 5 of 100

Figure 34. Cyber assets and Risk Assessment

The “Add Asset” button on the top right corner displays a modal window to the user, where they can add another asset for which a risk assessment will be performed (Figure 35).



Add Asset

Asset Name *

Name..

Description *

Description..

Criticality *

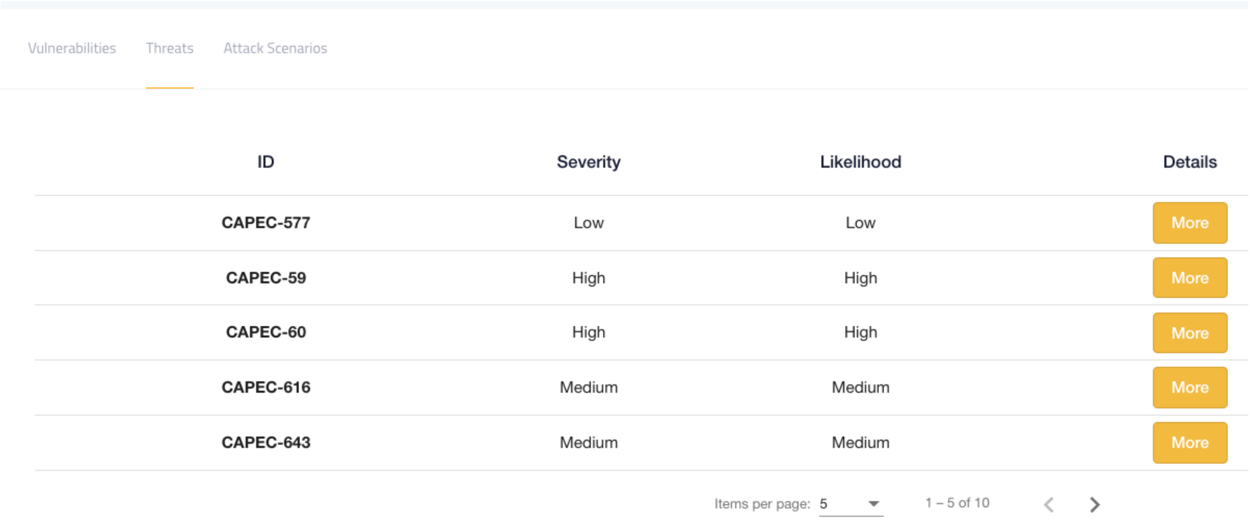
Criticality

Version *

Version

Figure 35. Adding a new asset to be assessed

The “More” button in the Actions section of a specific Asset redirects the user to a page where they can view the results from the risk assessment engine. More specifically, these are the risks (Vulnerabilities, Threats, Attacks scenarios columns) for a specific asset (Figure 36).



ID	Severity	Likelihood	Details
CAPEC-577	Low	Low	More
CAPEC-59	High	High	More
CAPEC-60	High	High	More
CAPEC-616	Medium	Medium	More
CAPEC-643	Medium	Medium	More

Items per page: 5 1 – 5 of 10

Figure 36. Risk assessment on a cybersecurity asset

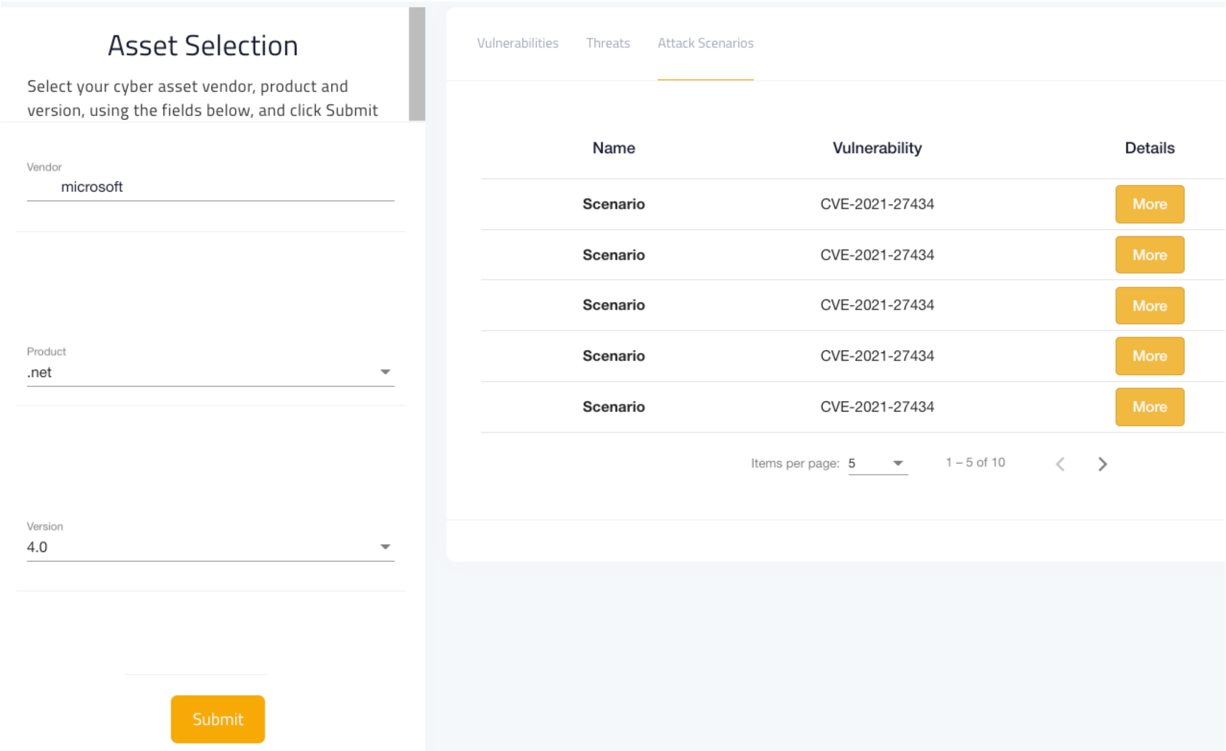
4.5.2 Measures

This part of the platform will be added in future versions.

4.5.3 Simulation Environment

Following this link, the user lands in a page where they can research vulnerabilities, threats and attack scenarios that the assets in their organization infrastructure may face (Figure 37). The user starts typing the first letters of the vendor of an asset and is presented with a list of potential vendors. After selecting one, the Product list below is dynamically populated with products of the specified vendor and in the same way as before, the user can start typing the first letters of a product. Similarly, after choosing one from the list, the Version dropdown is populated with the different versions of the specific product. Continuing, the user clicks “Submit” which retrieves all the relevant information from the database and fills in the three respective tables on the right-hand side (Vulnerabilities, Threats, Attack Scenarios), presented as tabs.

By clicking the “More” button of a specific entry in the table, a pop-up window is displayed (Figure 38) where the user can see more detailed information about it. In this way, the user can perform a security assessment of the organization’s infrastructure and learn about any relevant security gaps and threats that have already been identified by the international community.



Asset Selection

Select your cyber asset vendor, product and version, using the fields below, and click Submit

Vendor: microsoft

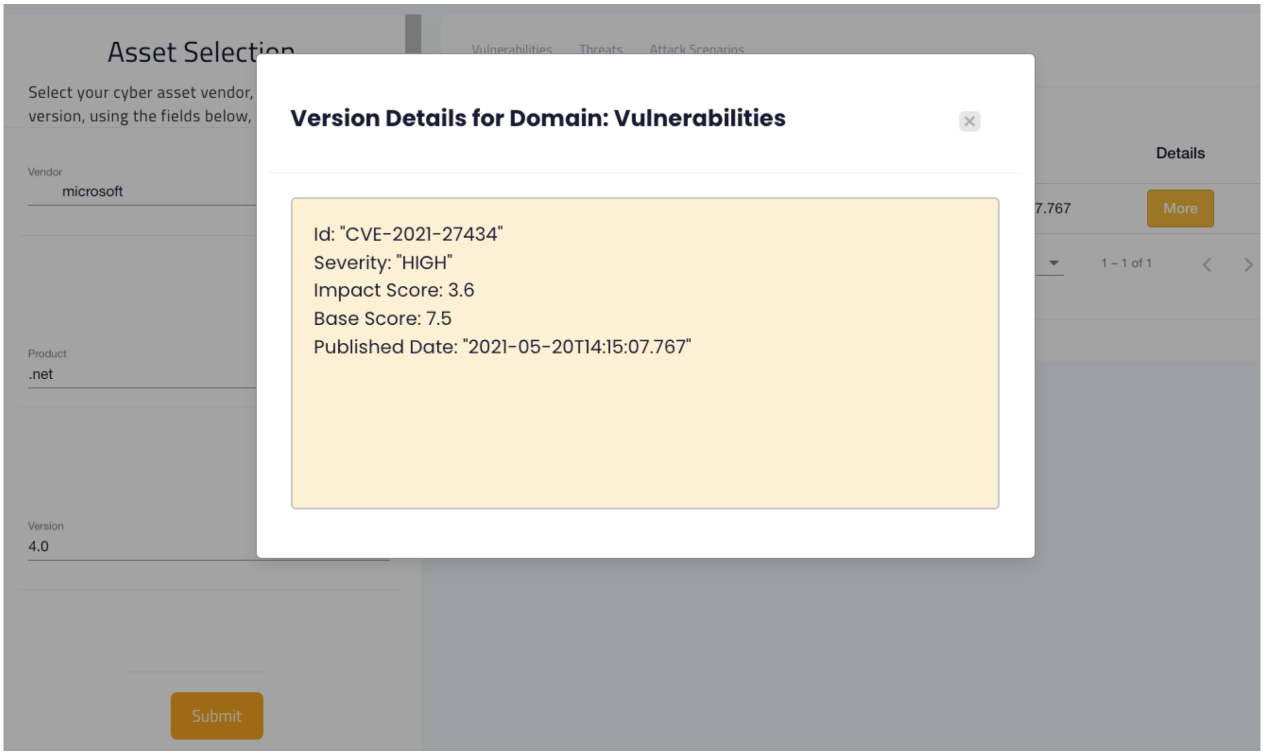
Product: .net

Version: 4.0

Name	Vulnerability	Details
Scenario	CVE-2021-27434	More
Scenario	CVE-2021-27434	More
Scenario	CVE-2021-27434	More
Scenario	CVE-2021-27434	More
Scenario	CVE-2021-27434	More

Items per page: 5 1 – 5 of 10

Figure 37. Cyber Security Self-Assessment Simulation Environment



Version Details for Domain: Vulnerabilities

Id: "CVE-2021-27434"
Severity: "HIGH"
Impact Score: 3.6
Base Score: 7.5
Published Date: "2021-05-20T14:15:07.767"

Figure 38. Details of a specific vulnerability

4.5.4 CyberRange

MySentinel offers a connection to the CyberRange platform, provided by Airbus CyberSecurity (Figure 39 and Figure 40). The CyberRange is a simulation platform that can be used either for testing systems before on-site integration or optimizing cyber-defence strategies or training end-users. When the user is redirected to the CyberRange platform, they have access to the SENTINEL Workzone. The user can, then, interact with the CyberRange-deployed Virtual Machine and Docker image, play actions or go through attack scenarios. For more information about the CyberRange, please refer to deliverable D4.2.

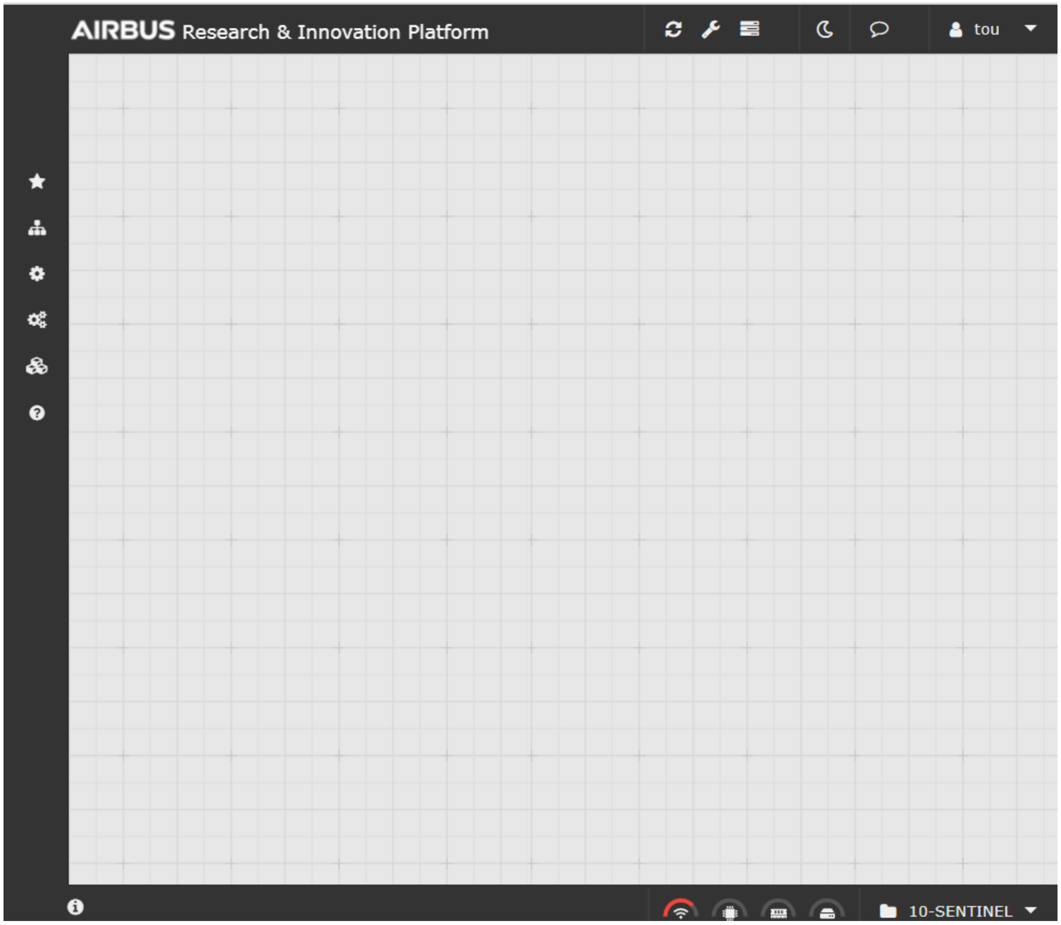


Figure 39. SENTINEL Workzone in the CyberRange platform (menu hidden)

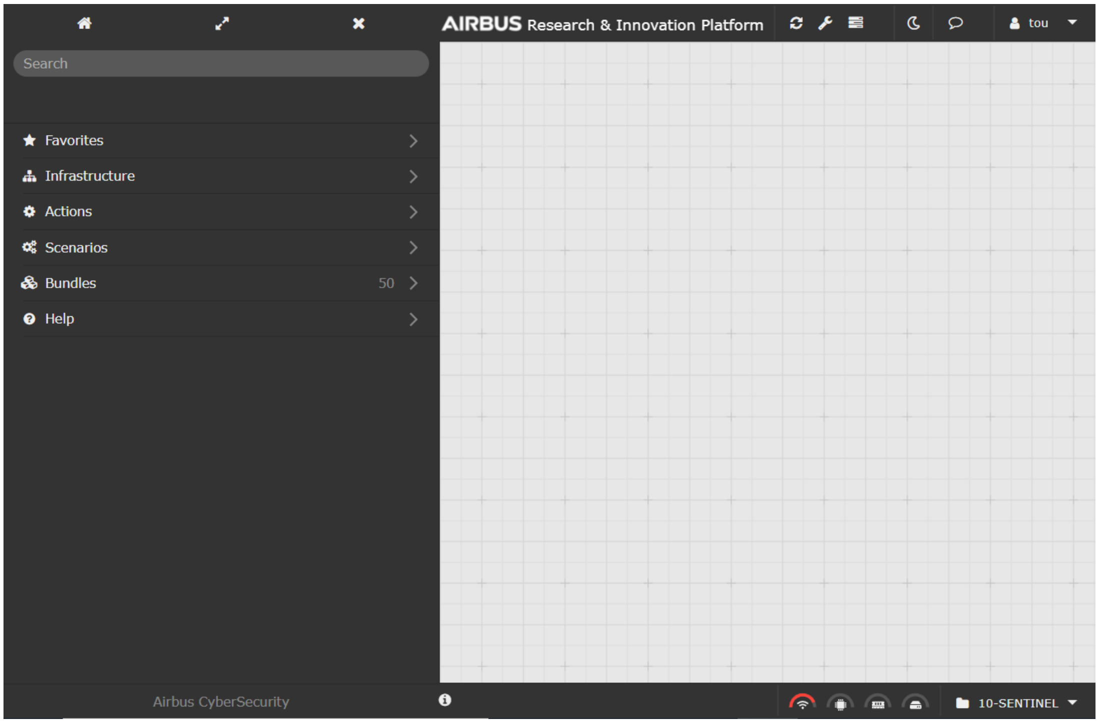


Figure 40. SENTINEL Workzone in the CyberRange platform (menu visible)

4.5.5 FVT

This part of the platform will be added in future versions.

4.6 Policy

By clicking on the ‘Policy’ menu item, the user is presented with the corresponding link “Recommendations” (Figure 41). More links will be added in future versions.

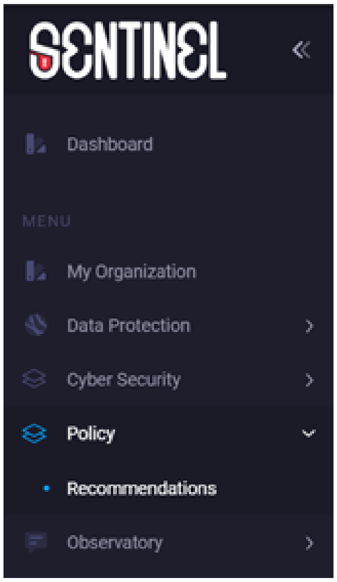
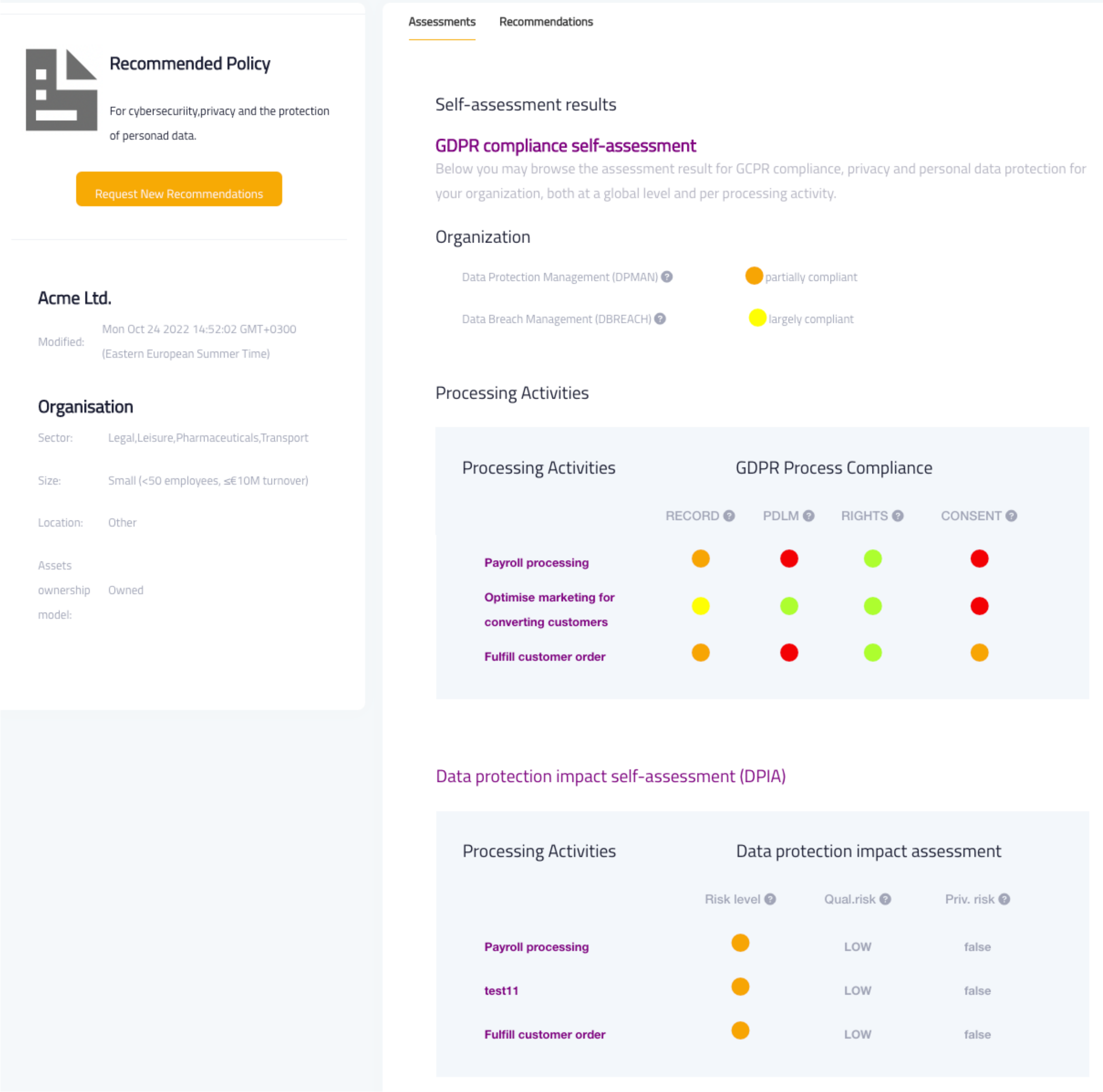


Figure 41. Policy Dropdown menu

4.6.1 Recommendations

This page has been updated since the last version reported on D5.1. Figure 42 presents the currently available assessments of the organisation together with the associated processing activities.



Recommended Policy

For cybersecuriity,privacy and the protection of personad data.

Acme Ltd.

Modified: Mon Oct 24 2022 14:52:02 GMT+0300 (Eastern European Summer Time)

Organisation

Sector:	Legal,Leisure,Pharmaceuticals,Transport
Size:	Small (<50 employees, ≤€10M turnover)
Location:	Other
Assets ownership model:	Owned

Self-assessment results

GDPR compliance self-assessment

Below you may browse the assessment result for GCPR compliance, privacy and personal data protection for your organization, both at a global level and per processing activity.

Organization

Data Protection Management (DPMAN)	🟠 partially compliant
Data Breach Management (DBREACH)	🟡 largely compliant

Processing Activities

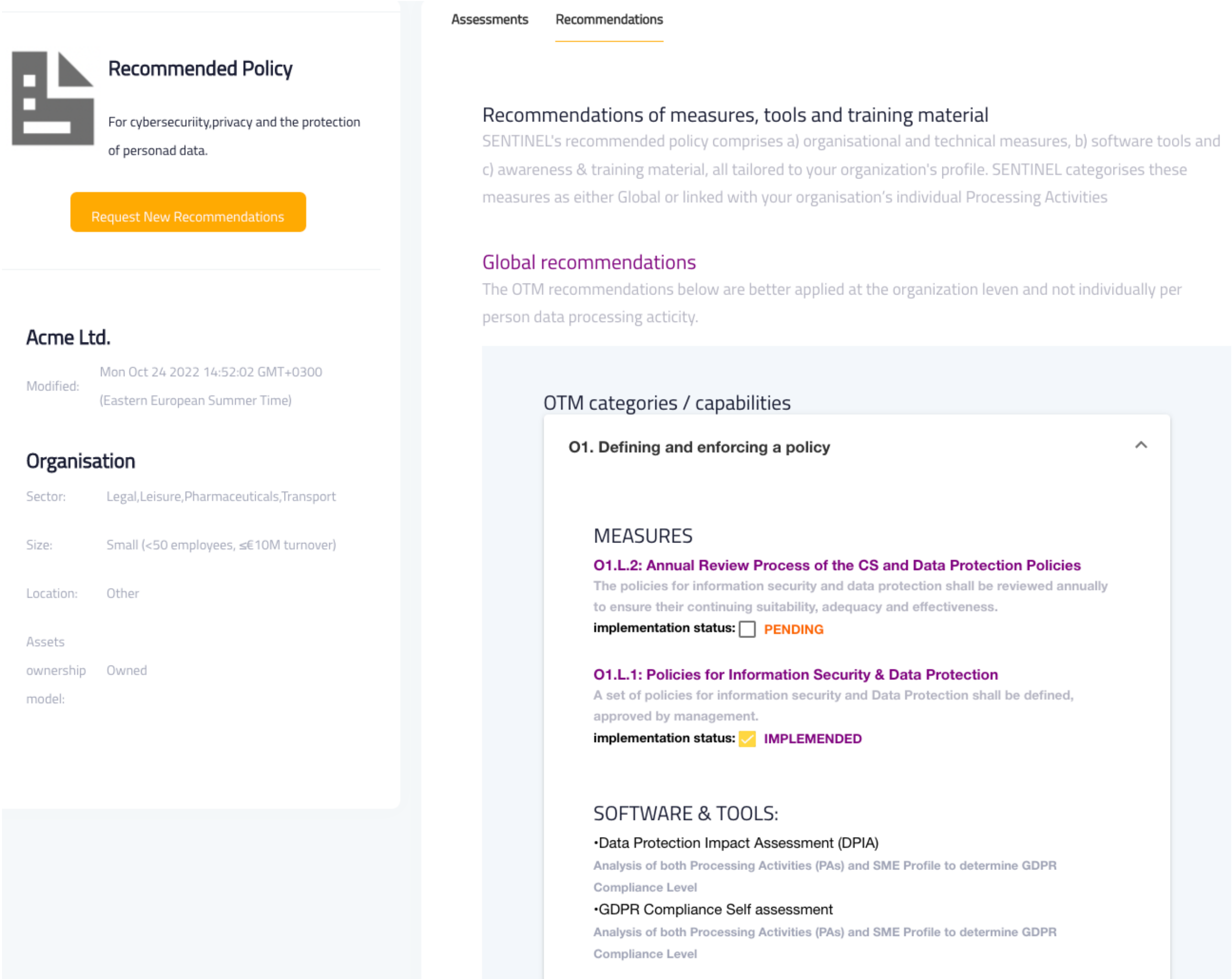
Processing Activities	GDPR Process Compliance			
	RECORD	PDLM	RIGHTS	CONSENT
Payroll processing	🟠	🔴	🟢	🔴
Optimise marketing for converting customers	🟡	🟢	🟢	🔴
Fulfill customer order	🟠	🔴	🟢	🟠

Data protection impact self-assessment (DPIA)

Processing Activities	Data protection impact assessment		
	Risk level	Qual.risk	Priv. risk
Payroll processing	🟠	LOW	false
test11	🟠	LOW	false
Fulfill customer order	🟠	LOW	false

Figure 42. Policy Page – Assessments

Moving on to the second tab, users can get the actual recommendations that SENTINEL proposes, according to the results found by the assessments. In this updated page, the user can see SENTINEL's recommended policy which comprises (a) a number of OTMs and (b) software tools (all categorised as either Global or linked to individual PAs), all tailored to their organization (Figure 43 and Figure 44). Here, the SME representative is able to provide an update to the system concerning the status of implementation of policies (Pending, Implemented) they have received as recommendations from the SENTINEL platform. This can be done via the checkboxes in the "Measures" section. Similar capabilities will be added for the other sections in future versions.



Recommended Policy

For cybersecuriity,privacy and the protection of personad data.

Acme Ltd.

Modified:	Mon Oct 24 2022 14:52:02 GMT+0300 (Eastern European Summer Time)

Organisation

Sector:	Legal,Leisure,Pharmaceuticals,Transport
Size:	Small (<50 employees, ≤€10M turnover)
Location:	Other
Assets ownership model:	Owned

Recommendations of measures, tools and training material

SENTINEL's recommended policy comprises a) organisational and technical measures, b) software tools and c) awareness & training material, all tailored to your organization's profile. SENTINEL categorises these measures as either Global or linked with your organisation's individual Processing Activities

Global recommendations

The OTM recommendations below are better applied at the organization leven and not individually per person data processing acticity.

OTM categories / capabilities

O1. Defining and enforcing a policy

MEASURES

O1.L.2: Annual Review Process of the CS and Data Protection Policies

The policies for information security and data protection shall be reviewed annually to ensure their continuing suitability, adequacy and effectiveness.

implementation status: □ PENDING

O1.L.1: Policies for Information Security & Data Protection

A set of policies for information security and Data Protection shall be defined, approved by management.

implementation status: ☑ IMPLEMENDED

SOFTWARE & TOOLS:

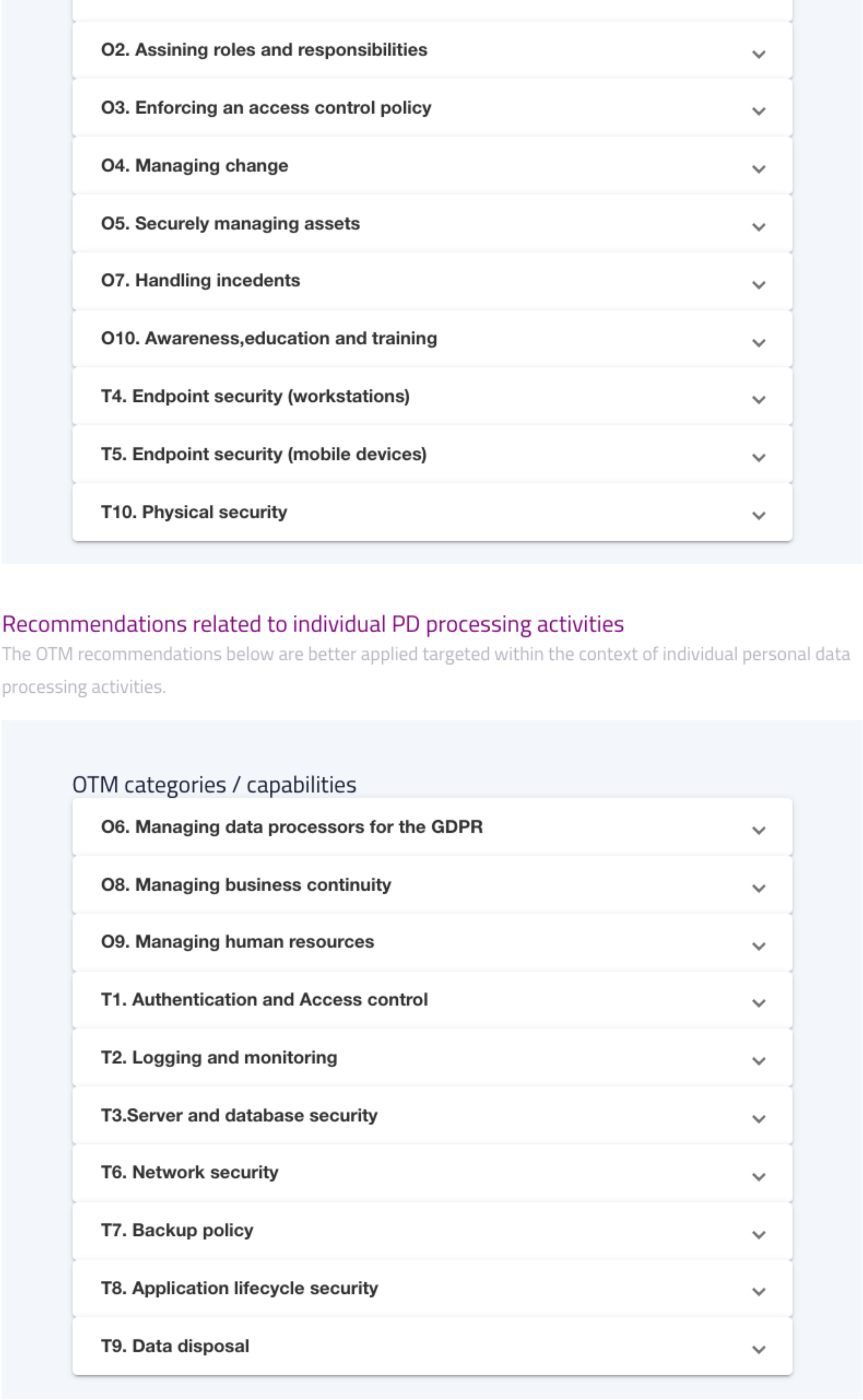
•Data Protection Impact Assessment (DPIA)

Analysis of both Processing Activities (PAs) and SME Profile to determine GDPR Compliance Level

•GDPR Compliance Self assessment

Analysis of both Processing Activities (PAs) and SME Profile to determine GDPR Compliance Level

Figure 43. Global policy recommendations (OTM1)



O2. Assining roles and responsibilities

O3. Enforcing an access control policy

O4. Managing change

O5. Securely managing assets

O7. Handling incedents

O10. Awareness,education and training

T4. Endpoint security (workstations)

T5. Endpoint security (mobile devices)

T10. Physical security

Recommendations related to individual PD processing activities

The OTM recommendations below are better applied targeted within the context of individual personal data processing activities.

OTM categories / capabilities

O6. Managing data processors for the GDPR

O8. Managing business continuity

O9. Managing human resources

T1. Authentication and Access control

T2. Logging and monitoring

T3.Server and database security

T6. Network security

T7. Backup policy

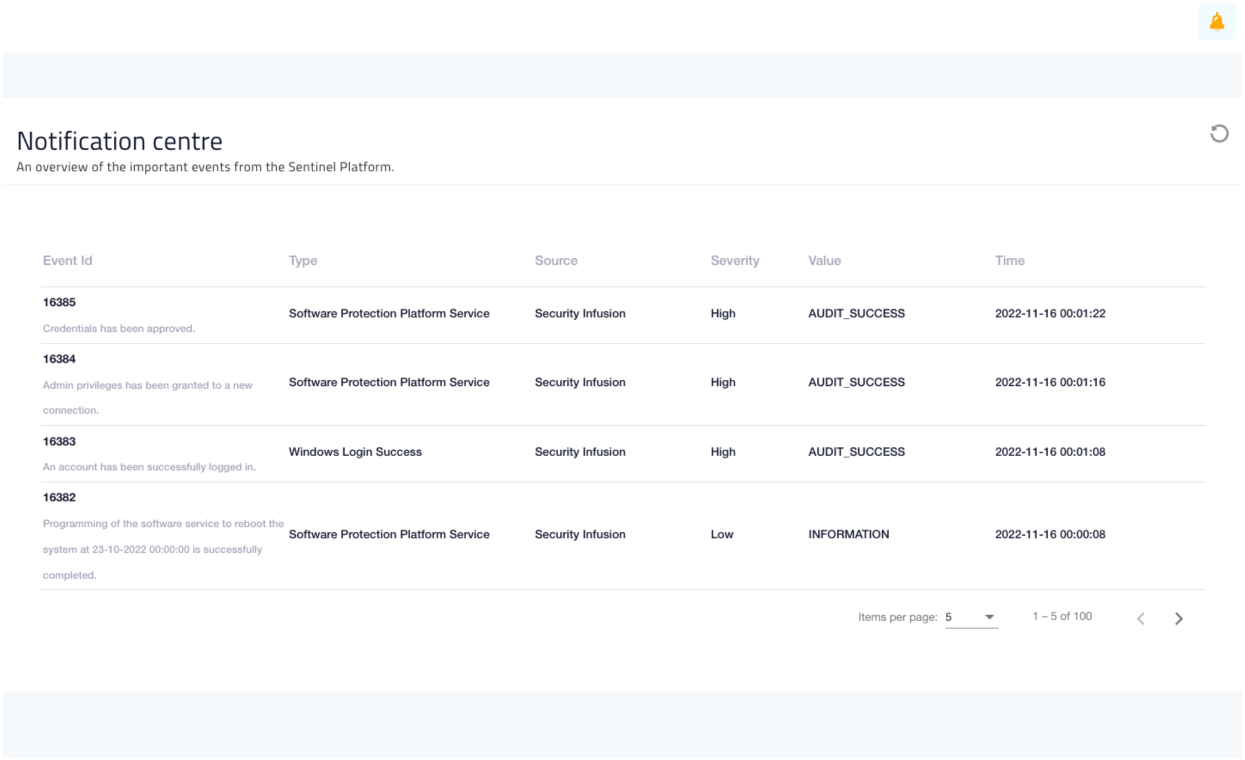
T8. Application lifecycle security

T9. Data disposal

Figure 44. Global policy recommendations (rest of OTMs) and individual PA recommendations

4.7 Security Notifications

There is no specific menu item link for the security notifications of the platform. Instead, there is a 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 (Figure 45). By clicking on it, the user moves to a page where they are able to see an overview of the important events from the platform. Additionally, there is a Refresh button just below the Bell, which the user can click in order to update the notifications manually. The reported events are being sent by the security plugins (for example Security Infusion) then collected by the Notification Aggregator and sent to the MySentinel UI.



Notification centre

An overview of the important events from the Sentinel Platform.

Event Id	Type	Source	Severity	Value	Time
16385 Credentials has been approved.	Software Protection Platform Service	Security Infusion	High	AUDIT_SUCCESS	2022-11-16 00:01:22
16384 Admin privileges has been granted to a new connection.	Software Protection Platform Service	Security Infusion	High	AUDIT_SUCCESS	2022-11-16 00:01:16
16383 An account has been successfully logged in.	Windows Login Success	Security Infusion	High	AUDIT_SUCCESS	2022-11-16 00:01:08
16382 Programming of the software service to reboot the system at 23-10-2022 00:00:00 is successfully completed.	Software Protection Platform Service	Security Infusion	Low	INFORMATION	2022-11-16 00:00:08

Figure 45. Notification Centre

All SENTINEL plugins utilize a plugin adapter. The plugin adapter “listens” for events that take place in the monitored infrastructure and then pushes them to the Notification Aggregator. The Notification Aggregator is the module responsible to store and to push the notifications to the MySentinel UI to be displayed to the user, as well as carry the logic to select which notifications are relevant to the specific user.

For the time being and as an example, we have selected specific relevant notifications (i.e. failed login attempts) from ITML’s Security Infusion to be displayed, but this list will be expanded to include other items related to infrastructure monitoring and overall system security.

More details on the functionality and integration of the module can be found in deliverables D3.2 and D5.5.

4.8 Observatory

The “Observatory” menu item currently includes the corresponding link “Knowledge Base” (Figure 46Figure 46). More links will be added in future version.

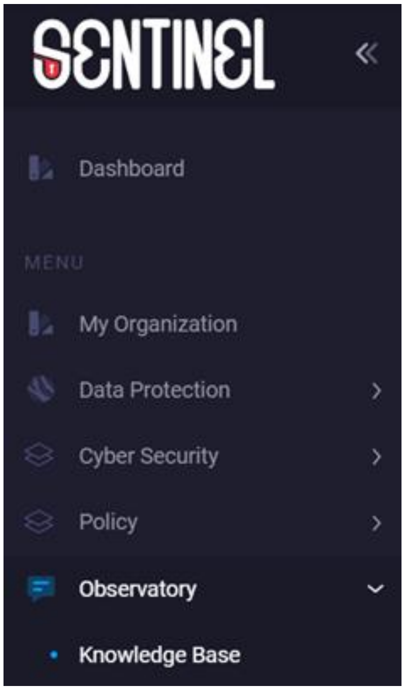
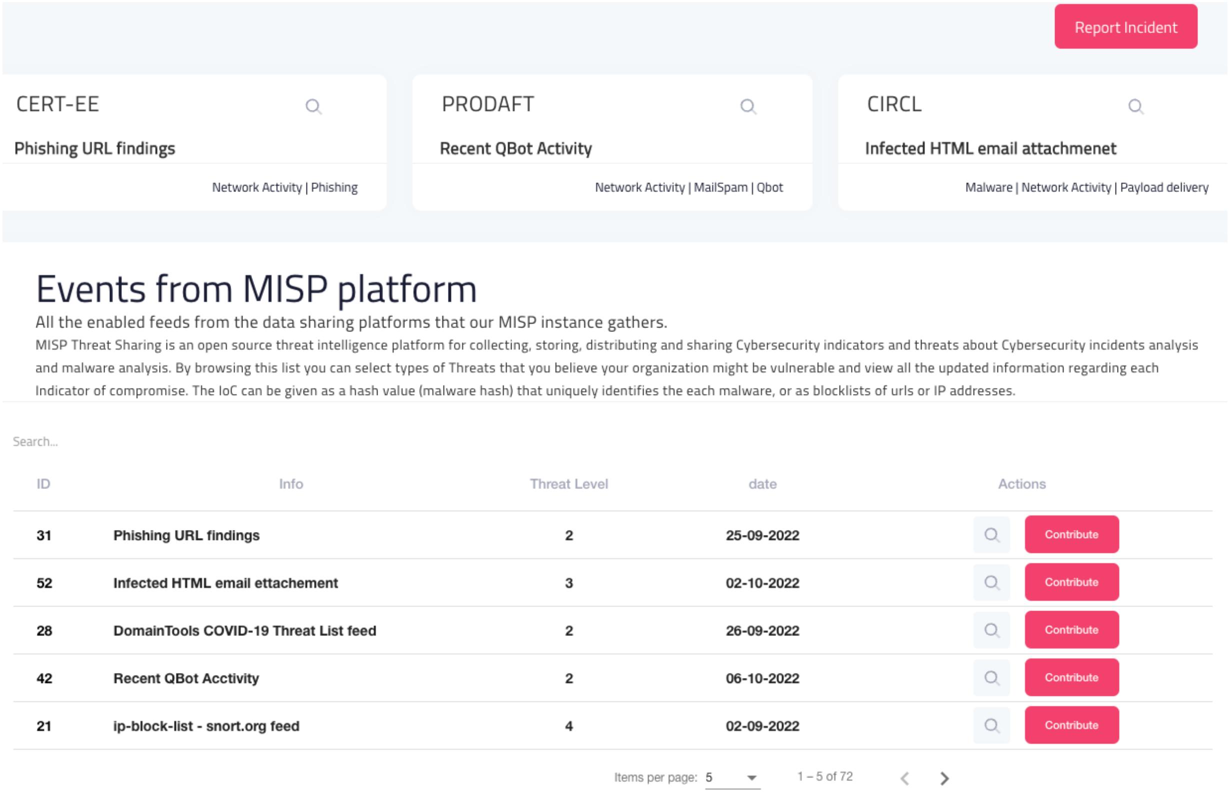


Figure 46. Observatory Dropdown menu

4.8.1 Knowledge Base

The Knowledge Base of SENTINEL’s Observatory provides the interface to the information collected via the activities performed in Task 3.1 “Access and monitoring of open data sharing platforms”. The Knowledge Base includes a list of threats (Figure 47) collected via the MISP instance used in the SENTINEL full-featured version. Detailed information on this can be found in deliverable *D3.2 “The SENTINEL digital core: Full-featured version”*.

Short descriptions are available on each page and on each feed the user is browsing, so that even non-technical users could navigate and find important information, articles, or to be informed for types of attacks that might affect their organisations. A search filter allows the users to select only specific information regarding the domain of their company. A vast variety of carefully selected feeds will be added on future versions that will include both purely technical and more simplified and informative events.



CERT-EE

Phishing URL findings

Network Activity | Phishing

PRODAFT

Recent QBot Activity

Network Activity | MailSpam | Qbot

CIRCL

Infected HTML email attachmenet

Malware | Network Activity | Payload delivery

Events from MISP platform

All the enabled feeds from the data sharing platforms that our MISP instance gathers.

MISP Threat Sharing is an open source threat intelligence platform for collecting, storing, distributing and sharing Cybersecurity indicators and threats about Cybersecurity incidents analysis and malware analysis. By browsing this list you can select types of Threats that you believe your organization might be vulnerable and view all the updated information regarding each Indicator of compromise. The IoC can be given as a hash value (malware hash) that uniquely identifies the each malware, or as blocklists of urls or IP addresses.

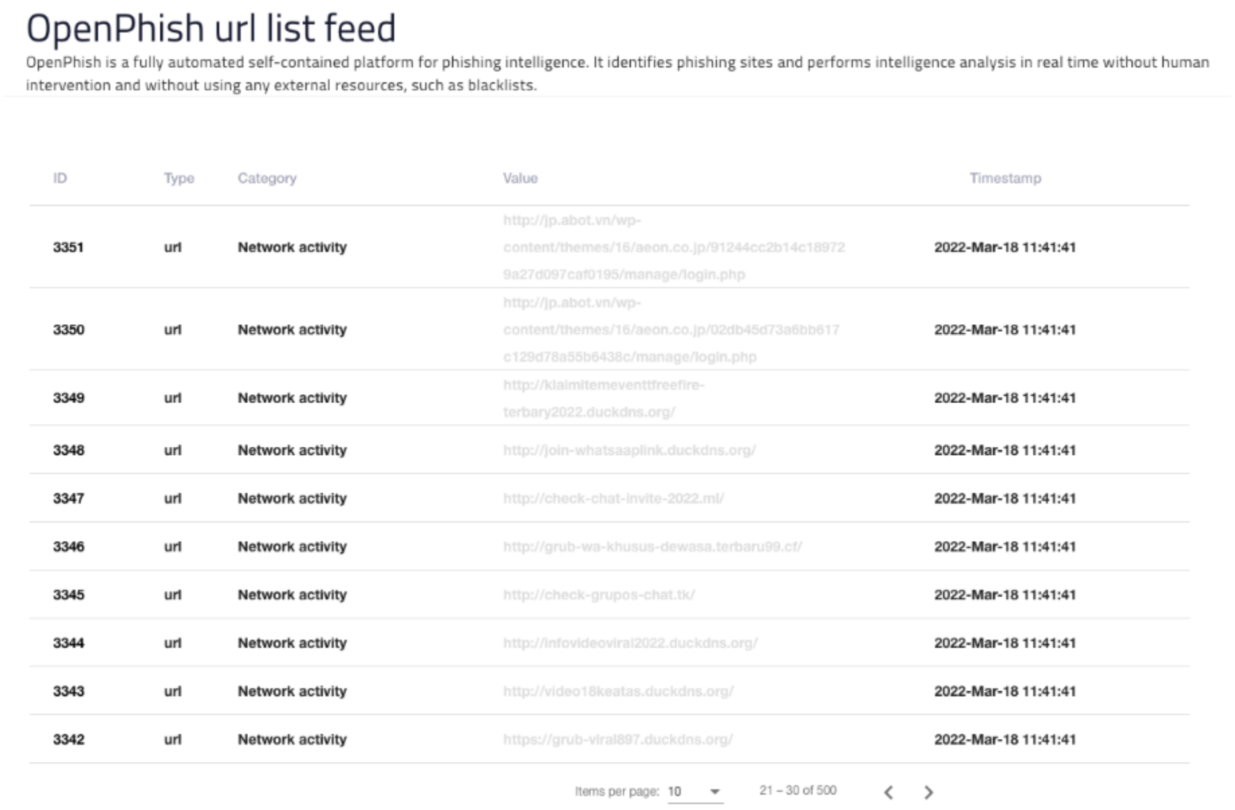
Search...

ID	Info	Threat Level	date	Actions
31	Phishing URL findings	2	25-09-2022	Contribute
52	Infected HTML email ettachement	3	02-10-2022	Contribute
28	DomainTools COVID-19 Threat List feed	2	26-09-2022	Contribute
42	Recent QBot Acctivity	2	06-10-2022	Contribute
21	ip-block-list - snort.org feed	4	02-09-2022	Contribute

Items per page: 5 1 – 5 of 72

Figure 47. Knowledge Base - Threats List

Clicking on the “View” icon of a feed, opens up a new page with a list of specific threats with their details including the type, category, value and creation timestamp of each associated threat indicator, as seen in Figure 48 below.



OpenPhish url list feed

OpenPhish is a fully automated self-contained platform for phishing intelligence. It identifies phishing sites and performs intelligence analysis in real time without human intervention and without using any external resources, such as blacklists.

ID	Type	Category	Value	Timestamp
3351	url	Network activity	http://jp.abot.vn/wp-content/themes/16/aeon.co.jp/91244cc2b14c189729a27d097caf0195/manage/login.php	2022-Mar-18 11:41:41
3350	url	Network activity	http://jp.abot.vn/wp-content/themes/16/aeon.co.jp/02db45d73a6bb617c129d78a55b6438c/manage/login.php	2022-Mar-18 11:41:41
3349	url	Network activity	http://klaimitemeventtfreefire-terbary2022.duckdns.org/	2022-Mar-18 11:41:41
3348	url	Network activity	http://join-whatsaaplink.duckdns.org/	2022-Mar-18 11:41:41
3347	url	Network activity	http://check-chat-invite-2022.ml/	2022-Mar-18 11:41:41
3346	url	Network activity	http://grub-wa-khusus-dewasa.terbaru99.cf/	2022-Mar-18 11:41:41
3345	url	Network activity	http://check-grupos-chat.tk/	2022-Mar-18 11:41:41
3344	url	Network activity	http://infovideoviral2022.duckdns.org/	2022-Mar-18 11:41:41
3343	url	Network activity	http://video18keatas.duckdns.org/	2022-Mar-18 11:41:41
3342	url	Network activity	https://grub-viral897.duckdns.org/	2022-Mar-18 11:41:41

Items per page: 10 ▾ 21 – 30 of 500

Figure 48. Knowledge Base - Threat Details Page

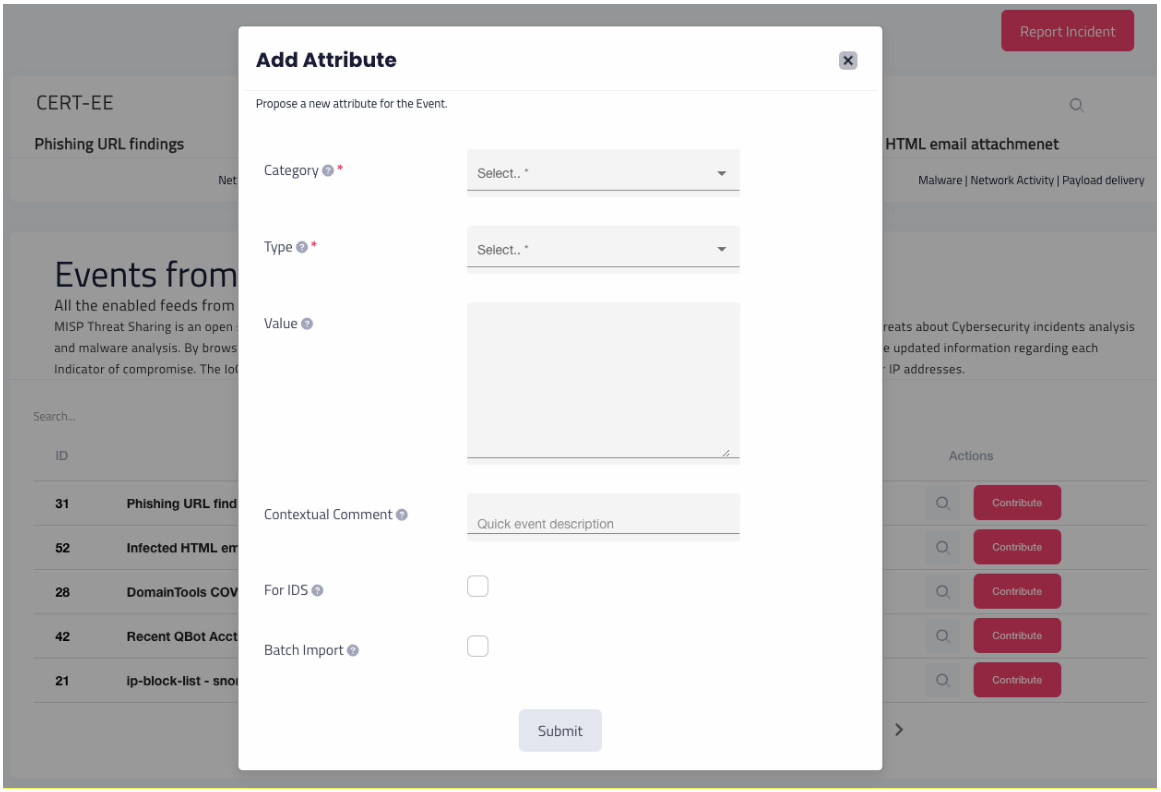
4.8.2 Incident Reporting Centre

The Incident Reporting Centre is another SENTINEL module that is new to the full-featured version. Similarly, to the security notifications of the platform, there is no specific menu item link for the Incident Reporting Centre. It is a part of the Observatory section of the platform (through the relevant menu link item).

This functionality allows the platform users to report incidents that have been observed in their organizations and register them in our threat intelligence sharing platform (MISP) to be readily available to all external users that subscribe to our MISP instance.

The user of the Observatory can either (i) add an incident to an existing event, or (ii) add a new event. In the first case, by clicking on the “Contribute” button of a specific event form the list, the user is called to fill in a standardized reporting form, as depicted in Figure 49. In the second case, the user can add a new event by clicking on the “Report Incident” button on the top right corner of the page and filling in the relevant form (Figure 50). Then, the data from either of these forms – through the Incident Broker – is reported to the Observatory Information Exchange module which in turn uploads it to MISP.

More information about contributing incidents back to the community can be found in deliverable D3.2.



Add Attribute

Propose a new attribute for the Event.

Category * : Select.. *

Type * : Select.. *

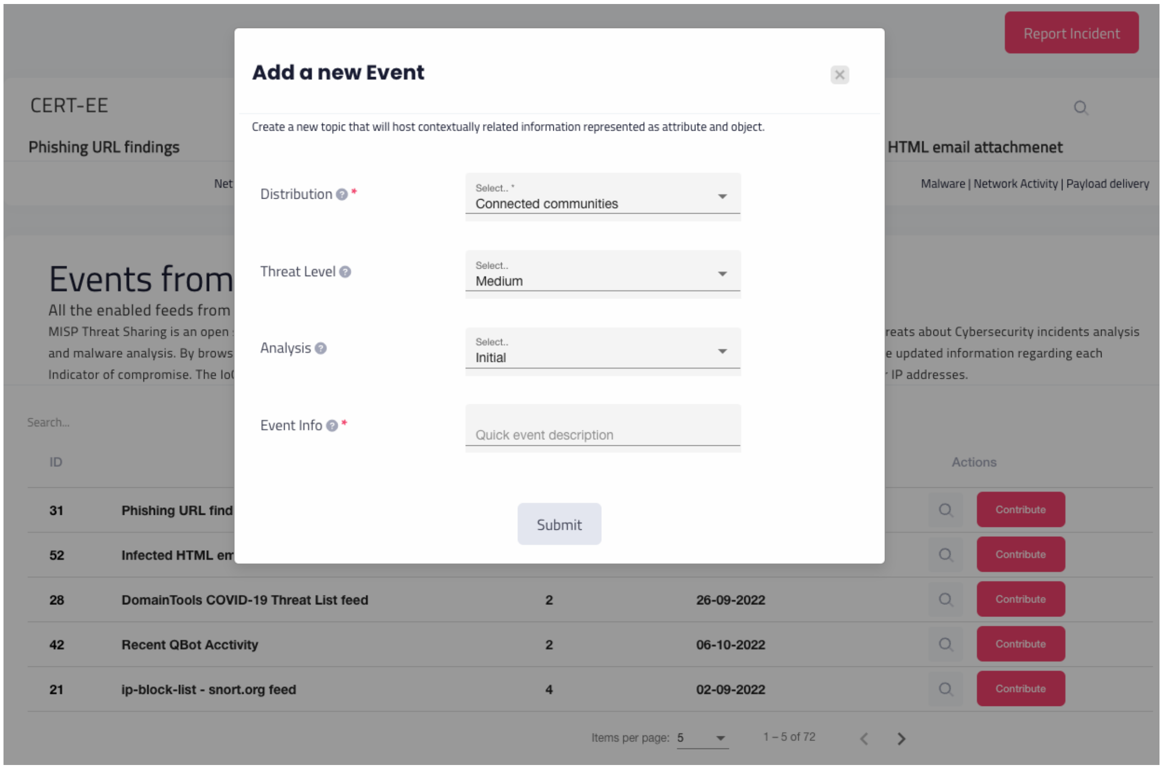
Value

Contextual Comment: Quick event description

For IDS □

Batch Import □

Figure 49. Adding an incident to an existing event



Add a new Event

Create a new topic that will host contextually related information represented as attribute and object.

Distribution * : Connected communities

Threat Level: Medium

Analysis: Initial

Event Info * : Quick event description

ID				
31	Phishing URL find			Contribute
52	Infected HTML em			Contribute
28	DomainTools COVID-19 Threat List feed	2	26-09-2022	Contribute
42	Recent QBot Acctivity	2	06-10-2022	Contribute
21	ip-block-list - snort.org feed	4	02-09-2022	Contribute

Items per page: 5 1 – 5 of 72

Figure 50. Adding a new event

5 Conclusion and Future Steps

This document presents the updates to the platform’s User Interface. The web application provides the user-facing part of the SENTINEL platform and intercommunicates with all the back-end components and modules, in order to offer the full SENTINEL functionality and experience to the end-user. The current version provides an update of the MVP release and includes all aspects of the platform that are present in the first complete prototype.

Additionally, to evaluate and further enhance the User Interface of the SENTINEL platform based on end-user experience, short-run experimentations on the SENTINEL MVP have been decided to carry out by the SENTINEL pilot owners. Aiming to deliver a user-centred design of the UI, we received feedback regarding the usability and overall user experience for MySentinel, from the pilot owners. As a result, we reveal opportunities to learn about users’ real needs and preferences (more information can be found in “D6.1 - SENTINEL Demonstration - initial execution and evaluation”). All the collected inputs were used to further improve and expand the UI. A similar process will take place for the upcoming version of the framework in parallel to real-life demonstration phase of the project. The UI will be updated and enriched in the final version, which will be documented in deliverable D5.3 (M30).