SENTINEL

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

D7.9 - Final business model, market analysis and long-term sustainability report

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.

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 7
Deliverable Title	D7.9 - Final business model, market analysis and long-term sustainability report
Version	2.1
Date of Submission	30/05/2024
Main Editor(s)	Marinos Tsantekidis, Costas Kalogiros (AEGIS)
Contributor(s)	Siranush Akarmazyan (ITML), Manolis Falelakis (INTRA), Yannis Skourtis (IDIR)
Reviewer(s)	Manolis Falelakis (INTRA), Yannis Skourtis (IDIR)

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

History			
Version	**Issue Date**	**Status**	**Distribution**
1.0	06/02/2024	ToC	Confidential
1.1	11/04/2024	Input to Sections 2 and 3	Confidential
1.2	16/04/2024	Input to Sections 2, 3 and 4	Confidential
1.3	19/04/2024	Input to Sections 2, 3 and 4	Confidential
1.4	23/04/2024	Input to Sections 2, 3 and 4	Confidential
1.5	26/04/2024	Input to Sections 2, 3 and 4	Confidential
1.6	08/05/2024	Input to Sections 2, 3 and 4	Confidential
1.7	10/05/2024	Input to Sections 3 and 5	Confidential
1.8	14/05/2024	Released for internal review	Confidential
1.9	20/05/2024	Review conducted by IDIR, INTRA	Confidential
2.0	27/05/2024	Reviewers' comments addressed	Confidential
2.1	30/05/2024	Final version ready	Public

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
ATP	Advanced Threat Protection
BFSI	Banking, Financial Services, and Insurance
Bn	Billion
CAGR	Compound Annual Growth Rate
CS	Cybersecurity
DESI	Digital Economy and Society Index
DFB	Data Fusion Bus
DNS	Domain Name System
DSM	Digital Single Market
DoA	Description of Action
DPO	Data Protection Officer
DPIA	Data Privacy Impact Assessment
DX.X	Deliverable X.X
FVT	Forensics Visualisation Toolkit
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GDPR CSA	GDPR Compliance Self-Assessment
ICT	Information and Communication Technology
IdMS	Identity Management System
IE	Information Exchange
IoT	Internet of Things
IT	Information Technologies
KB	Knowledge Base
KPI	Key Performance Indicator
MEs	Micro Enterprises
Mn	Million
NFBS	Non-Financial Business Sector
NGFW	Next-Generation Firewall
NGO	Non-Governmental Organisation
OECD	Organisation for Economic Co-operation and Development
OTMs	Organisational and Technical Measures
PA	Processing Activity
PEST	Political, Economic, Socio-cultural and Technological
PDP	Personal Data Protection
RE	Recommendation Engine
SI	Security Infusion
SIEM	Security Information and Event Management
SMEs	Small-Medium Enterprises
SSE	Security Service Edge
SSO	Single Sign-On
SWOT	Strengths, Weaknesses, Opportunities, and Threats
USD	United States Dollars
WPX	Work Package X
YoY	Year-over-year

Executive Summary

This deliverable provides a detailed market analysis for the Cybersecurity & Data Protection SME market and the final SENTINEL business model. It defines the current and expected market and stakeholder requirements to facilitate the commercialisation of SENTINEL.

This report is the final step to a complete business model for the SENTINEL project. The study and understanding of the possibilities of the cybersecurity and data protection market, as well as an unambiguous competitive analysis, will lay a strong foundation for the product to enter the market with traction which can be maintained in the long run, by highlighting characteristics that, according to the present study, will be prove SENTINEL's competitive advantage.

This deliverable's analysis will confirm the needs of the market which SENTINEL aspires to address. Furthermore, as part of SENTINEL's analysis of potential market targets, a concrete business model is formulated that could make SENTINEL's solution viable and competitive.

The purpose of this deliverable is to (a) assist the consortium in deciphering SENTINEL's market and (b) to identify the offering's strengths and weaknesses, as well as the market's opportunities and threats, as well as characteristics of the competition, so that it can guide the consortium during commercialization.

1. Introduction

1.1 Purpose of the document

This report presents the final market and stakeholder analysis as well as the concrete business plan that may exploit SENTINEL. This encompasses the identification of the intended and addressable market in terms of size and its trends, the key drivers and the regulations, incentives and legal aspects that define the business environment which SENTINEL aspires to enter. Additionally, it assesses the roles, expectations, and potential benefits of different stakeholders to understand how to leverage them, as well as SENTINEL's competitive environment. The analysis of the current and expected markets and stakeholder requirements and benefits will help the consortium implement the business plan and steer the product in the long term.

This document provides information towards refining market placement, including financial aspects (costs, revenues, pricing), as well as identifying suitable exploitation strategies for each application and context. Therefore, this report provides the final step in developing the business requirements and business model in SENTINEL. The understanding of the potential of the Cybersecurity & Data Protection market and the competition landscape gives the SENTINEL consortium great insights for the long-term sustainability and commercialization uptake to the primary market segments. This deliverable presents the culmination of the relevant processes that took place throughout the duration of the project.

1.1.1 Contribution to WPs and project objectives

This deliverable is composed in the context of Work Package (WP) 7 "Ecosystem building, Exploitation and sustainability management" and constitutes the final output of Task 7.1 "Market continuous analysis and business planning for SENTINEL exploitation", as presented in the Description of Action (DoA) that provides support to the WP7 following objective:

Objective 5: Develop the SENTINEL business model and strategies for incentivising/promoting project adoption by various stakeholders within the SMEs/MEs ecosystem during and after the project.

As a result, this deliverable contributes to the work performed within WP7 from the business modelling perspective. It concludes the efforts in this respect, as the succession of D7.2 "Market analysis and preliminary business modelling" delivered on M6 and D7.7 "Exploitation strategy, standardisation activities and best practices - interim version" delivered on M18 (where an intermediate business plan was presented).

Combining the results of this study with the results of WP6 "Real-life experiment evaluations: SENTINEL pilots" we are able to match the final product to the market needs and create a strong application that gives solutions to critical cybersecurity & data protection issues for SMEs in Europe.

1.2 Structure of the document

The rest of the document is structured as follows:

- **Section 2** revisits and updates aspects of the market analysis methodology that was presented in D7.2, for the sake of completeness.
- **Section 3** focuses on the security and data protection market, presenting the market outlook and highlights the main industry challenges and opportunities that drive the market potential.
- **Section 4** presents an analysis of competitors in the security and data protection market.
- **Section 5** identifies the SENTINEL competitive advantage, including the PEST and SWOT analyses.
- **Section 6** details the business model of the SENTINEL platform, containing cost, revenue and price modelling.
- **Section 7** concludes the deliverable

1.3 Intended readership

This document is primarily addressed to members of the project consortium, while it may also serve as informative market insight for any external party.

2. Market Analysis Methodology

In this section, for the sake of completeness, we present the market analysis methodology that we laid out in and followed since D7.2 “Market analysis and preliminary business modelling”.

2.1 Overview of the SENTINEL concepts

SENTINEL addresses the challenges and needs related to personal data protection that currently European SMEs/MEs face [29]; these primarily concern awareness of GDPR and other data protection-relevant legislative framework, high-entry points to obtain enterprise-grade security and personal data protection and rise in IT infrastructure complexity. SENTINEL addresses these challenges for European SMEs/MEs, by raising awareness and boosting their capabilities in the domain through innovation at a cost-effective level. This is realized by offering digital tools, a methodology and archetypal solutions.

SENTINEL encompasses a list of components and plugins (an extensive list is provided as part of D1.1 “The SENTINEL Baseline” and D1.2 “The SENTINEL technical architecture”) that were further developed under WPs 2, 3, 4 and integrated into a common framework under Work Package 5. They are categorized as follows:

- Core modules, which are grouped in four (4) Contexts and effectively constitute the SENTINEL platform architecture.
- Internal plugins, which are contributed or developed by SENTINEL partners, comprising services and functionalities for SMEs.
- External plugins and trainings, which may be recommended to SMEs, selected from an open and non-exhaustive list.

The four (4) contexts of SENTINEL include:

- My SENTINEL: It includes the SENTINEL UI and dashboard. 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 status by presenting every connected service.
- Self-Assessment: It includes the *SENTINEL Self-Assessment Service* responsible for assessing the risk score of both the organisation and its processing activities (PAs) and the *Profile Service* which stores organisation profiles and provides persistence for storing and fetching organisation and PA data.
- Core: It includes the *Recommendation Engine* responsible for producing a list of recommended plugins, trainings and Organisational and Technical Measures (OTMs) that address the specific security and data protection profile of an organisation. It also includes the *Policy Drafting Engine* that enhances the plugin recommendations with related trainings and drafts a comprehensive security policy for the SME and *Policy Monitoring and Enforcement Engine* that tracks the implementation status of the policy recommendations contained in the policy draft.
- Observatory: It includes the Observatory Knowledge Base (KB) and the Information Exchange (IE) modules, that enable the exchange of critical data and knowledge over threats, signatures and evidence as well as anonymised policy drafts between the SME and open security data sharing platforms. Reporting data and privacy breaches and

incidents to open-source incident response platforms (as handled by SENTINEL's incident reporting components) as well as the continuous monitoring of such open data sets, is an additional pivotal goal of the Observatory IE, ensuring a continuous aggregation of information for the SENTINEL KB.

SENTINEL plugins

The following Plugins have been integrated into the SENTINEL platform providing different capabilities:

- ***GDPR Compliance Self-Assessment (GDPR CSA)*:** GDPR CSA is designed to support SMEs/MEs to be accountable regarding the processing of personal data by helping them to identify what are the requirements to meet to process personal data, check that Organisational or Technical Measures (OTMs), and identify what and how to improve accountability.
- ***Security Infusion (SI):*** SI offers holistic IT event management and cybersecurity risk mitigation. It is used as part of the "Receive Security Notifications" use case. Agents can be installed on the premises of one of the SENTINEL partners and monitor pre-determined parts of its infrastructure.
- ***Identity Management System (IdMS):*** It delivers a solution that enables the creation of centralized, trusted digital identities for individuals, relates these identities with specific roles and access rights, and finally uses these identities to securely leverage both user data and SME data, so SENTINEL participants may be GDPR compliant in terms of data portability and data sovereignty.
- ***MITIGATE*:** Offers multi-order and impact assessment capabilities for identifying/assessing risks, threats and incidents and estimates their impact in interdependent infrastructures. It promotes collaboration among business entities in assessing and exploring their risks allowing them to manage their cybersecurity in a holistic and cost-effective manner.
- ***Data Protection Impact Assessment (DPIA):*** It provides the capability to execute data protection impact self-assessments and is designed to allow SMEs to identify (through assessment) the risks associated with their personal data processing activities. The carrying out of a DPIA is demarcated as *mandatory* in SENTINEL, for Processing Activities which, according to the Self-Assessment Engine, are scored as likely to result in high risks to individuals' data privacy
- ***CyberRange***: provides (a) gamified training and educational content to raise awareness of cybersecurity and data protection best practices and (b) the ability for SMEs to test, evaluate, and train in real-world cyber threat scenarios.
- ***Forensics Visualisation Toolkit (FVT):*** offers a complete toolset for IT security data collection, processing, and visualization.

External Plugins and Trainings

Apart from its own mechanisms, the SENTINEL platform can also suggest to the user external open-source tools and training to fill the identified gas. Therefore, a wide list of **54 free and/or** open-source tools is established. These solutions cover all the OTM capabilities that are subject to the SENTINEL methodology. Furthermore, the SENTINEL platform can suggest relevant external training resources that can aid the user in enhancing their overall privacy and security

stance. An extensive compilation of **117 training components** has been assembled, encompassing all aspects considered by the SENTINEL methodology. The training materials encompass a wide array of topics, including but not limited to privacy, security, the intersection of privacy and security, safety, ethics, and the implications arising from cutting-edge technologies like Artificial Intelligence (AI), the Internet of Things (IoT), Big Data, surveillance systems, among others.

2.2 Methodology for analysing the SENTINEL market

To ensure full coverage of industry viewpoints, the approach used in this report necessitated an elaborate research framework. Important discoveries were gained from a mixture of many models utilized to gain a thorough grasp of the target markets in order to achieve this. The SENTINEL consortium has used the three insight perspectives listed below:

- *The Market insights perspective*, which involves studying publicly available industry reports for identifying long-term and emerging macroscopic market trends, including estimates about market size evolution, market challenges and business opportunities in the domain of cybersecurity and data protection.
- *The Competition insights perspective,* which attempts to list key competitors and their offerings with emphasis on existing and planned features, market share, as well as strengths and weaknesses for incumbent players and the competitive landscape of start-ups.
- *The Client insights perspective*, which targets the key activities that the main intended user groups seek to perform and better understand their existing pain points, as well as the expected gains by adopting SENTINEL approach.

Each one of these three perspectives has been closely monitored and updated since their preliminary version included in the first version of this document (i.e. D7.2 “Market analysis and preliminary business modelling”). With this analysis framework, SENTINEL is able to identify the drivers of targeted sectors and domains, the needs and expectations of targeted end-users, and the overall potential to enter the market and to identify the associated competing products. Via the market analysis, critical aspects, opportunities, influencing factors and relevant actors are identified, in order to better place the final SENTINEL offered product in the market.

2.3 Market analysis planning

In this section, we detail the work plan and the activities for the three perspectives comprising the SENTINEL market analysis methodology that we introduced in the previous section and we followed throughout the duration of the project.

The implementation of the market analysis methodology follows a four-phases approach for the identification of the market segments and the detailed planning of the exploitation activities. In this approach, we step on the project general scope, the business objectives, and the expected outcome, as they were introduced in Section 2.1, in order to position the results of SENTINEL in the target market segments and develop a solid business plan and go-to-market strategy. These phases of the market analysis methodology are:

Phase 1 (M1 - M6): Establish a common understanding of the expected project outcome with respect to the key market innovations that we wanted to develop and the business stakeholders

that were intended to use these innovations. Expected outcome: Through analysing and sizing the Cybersecurity & Data Protection market and the position of SENTINEL with the respect to the existing solutions and their maturity, this phase resulted in the definition of the SENTINEL value and unique selling proposition (please refer to D7.2 “Market analysis and preliminary business modelling” and D7.7 “Exploitation strategy, standardisation activities and best practices – interim version”).

Phase 2 (M7 - M18): Based on the progress and the results of Phase 1, consortium partners defined a coherent exploitation strategy that describes the pathway of the exploitation of the identified assets. Moreover, the defined dissemination and communication strategy boosted the awareness level of targeted stakeholders, facilitating the standardization activities of SENTINEL. The results of this phase are reported in D7.7 “Exploitation strategy, standardisation activities and best practices – interim version” delivered on M18.

Phase 3 (M19 - M24): Prepare the pathway for exploitation and feed the business planning and modelling activities towards the commercialisation of SENTINEL. Expected outcome: Update the target market segments, and the intended business stakeholders and relevant market representatives to approach, as well as analyse the existing business models and pricing strategy. This phase will be explained in the rest of this section across the three adopted models.

Phase 4 (M25 - M36): Following the progress made in the previous three phases, a solid business plan and go-to-market strategy were developed during this stage, considering the present market situation as well as legal and regulatory constraints. In addition, the consortium ensured that the monitored KPIs presented in Table 1 were met and an impact assessment delivered. The results of this phase are reported in the present document D7.9 “Final business model, market analysis and long-term sustainability report”, in conjunction with D7.8 “Exploitation strategy, standardisation activities and best practices – final version”, as well as D8.3 “Yearly project management report - third version”, all delivered on M36.

2.3.1 Market insights

This literature review aims to cover the scope of the project and presents the current maturity of the broader market of cybersecurity, personal data protection and GDPR compliance domain. The activities in the implementation of this insight step on top of the current trends and dynamics of each market in scope and elaborate on the following:

a) identifying markets main drivers and constraints
b) identifying emerging technologies and trends that may impact the markets
c) finetuning our offerings to better serve potential customers
d) identifying risk mitigation strategies

To achieve the aforementioned activities, the project performed extensive desk research in order to ascertain the material in the public domain both within the academic and grey literature. The majority of the reports gave high-level opinions and trends about the evolution and the dynamics of each market on a global level. Due to the novelty and sensitivity of this area, many of the industry opinions and recent developments were not in the public domain. This illustrates the need for combining the results of this perspective with the Client/Experts insight perspective.

The execution of the activities in this model spans the project's lifetime, with emphasis on the second and third year of the project, which have set the baseline for business planning and commercial exploitation. Within this period, the following activities were refined:

- Revise and expand the initial market considerations as presented in the Description of Action, with the aim to drive the positioning of the project to the general market environment, and
- Update the market trends and assumptions, based on the project developments and the evolution of the targeted market throughout the project duration, in order to meet the evolving needs and expectations of the targeted end-users.

2.3.2 Competition insights

The purpose of the competitive insight's viewpoint is to evaluate the strengths and shortcomings of existing and prospective SENTINEL competitors. In order to identify opportunities and risks, the relevant analysis gives both an offensive and defensive strategic perspective. Profiling combines all of the relevant sources of competitor analysis into one framework in the support of efficient and effective strategy formulation, implementation, monitoring and adjustment. Competition insights, in combination with market insights and experts' opinions provide valuable inputs for the strategic SENTINEL positioning in the competitive vertical markets that next-generation applications rely on.

The main activities of this model occur through desk research, in which we put an emphasis on listing indicative solutions, products, services and business strategies of other initiatives that bear similarity to SENTINEL's objectives. Additionally, competition has been monitored throughout the project's lifetime and the results of these activities are documented in this deliverable.

2.3.3 Client & Expert insights

To build upon the desk research activities regarding the market and the competition landscape insights, this perspective brings into the project the knowledge and expertise of the consortium members and the industry professionals in the field of cybersecurity and data protection continuum for a variety of business domains, with an emphasis on application areas, as they are represented by the use case providers that participate in the SENTINEL project.

To achieve this, a set of interaction sessions with SENTINEL contributors and early adopters were planned, aiming to build a common vision among the industrial partners on the market segments that the SENTINEL framework targets. The activities in this model have enabled the creation of an inventory with key trends. Such trends and innovations, in terms of technological advances and business priorities, have driven the specification of the key capabilities of the framework and their adoption scenarios, connecting the activities in the market analysis with the specification of the SENTINEL architecture and the development of the project exploitation roadmap.

This model has evolved in two phases: a) Phase A, which targeted mainly the consortium partners to provide their view on the market directions of the SENTINEL solution, and b) Phase B, in which the experts and stakeholders that are involved in the first and second evaluation phase of the SENTINEL prototype were also be asked to provide their perception on the market potentials of the SENTINEL, especially in the specification of the business modelling opportunities. The set-

up of the activities in phase B is implemented in the context of D6.3 “Assessment report and impact analysis”, which is due on M36.

In order to structure the interactions with users in the clients’ and experts’ insights perspective, a list of questions is used, as the basis for deliberation and discussion with them. Part of these questions were used in phase A to facilitate the organization of group discussions with the involvement of all SENTINEL partners. Specifically, within WP7 activities a dedicated questionnaire was formed to set a framework of questions with the overall aim to investigate and form a common understanding of the SENTINEL environment, regarding the value we offer, the competition we may face and our future marketization. The questions asked were designed either to fill gaps from the literature or to gain insight into the interviewees’ understanding of the market and any perspectives on potential areas of opportunity.

2.4 KPIs definition and monitoring

In order to maximize its benefits to SMEs/MEs and, indirectly, to the general public, SENTINEL assures a multimodal set of impacts. Its maximization strategy ensures openness, sustainability, and ecosystem participation, and validates the delivery of impacts via quantifiable Key Performance Indicators (KPIs) with defined goal values and ways of verification directly related to its workplan. Table 1 lists the relevant KPIs and their status at the end of the project. More details can be found in deliverable D8.3 “Yearly project management report - third version”

Table 1. SENTINEL Impact KPIs

iKPI	Description	Status
iKPI 1.1	At least four (4) privacy and personal data protection technologies delivered	Achieved
iKPI 1.2	At least six (6) standards, regulations and directive incorporated within SENTINEL	Achieved
iKPI 1.3	At least 40% improved privacy compliance efficiency for SMEs/MEs	Achieved
iKPI 2.1	More than 20 entities CERTS / CSIRTS engaged by the end of the project	Achieved
iKPI 2.2	More than 8 Digital Innovation Hubs engaged by the end of the project	Achieved
iKPI 2.3	More than 20 novel services, tools and modules within the SENTINEL platform	Achieved
iKPI 3.1	At least three (3) improved business models developed within the SENTINEL project	Achieved
iKPI 3.2	At least 40% reduction of compliance – related costs	Achieved
iKPI 4.1	At least 4 tools reach market readiness level eight (8)	Achieved
iKPI 4.2	More than 10 critical aspects addressed to ensure long-term sustainability	Achieved
iKPI 4.3	10.000 smaller enterprises entities and third parties reached	Achieved
iKPI 9	At least four (4) innovative technologies advanced within SENTINEL	Achieved
iKPI 10	At least five (5) cases testing and validating the innovative capacity of the SENTINEL’s offerings	Achieved

iKPI 11.1	At least 20 third-party entities (SMEs/MEs) directly using SENTINEL's tools/services	Achieved
iKPI 11.2	At least 10% increase of market share for SMEs/MEs exploiting SENTINEL	Partially achieved
iKPI 12.1	At least four (4) start-ups and spin-offs boosted exploiting SENTINEL security services	Achieved
iKPI 12.2	At least 15% increase in sales for the pilot partners exploiting the SENTINEL platform	Partially achieved

3. The Cybersecurity & Data Protection Market

3.1 Market definition

A thorough comprehension of the market in which players compete is seen as necessary before describing the financial drivers for product or service providers to innovate and achieve market breakthroughs. Such innovations also require a relatively deep understanding of the potential horizontal and vertical segmentation of the market as well as the overall policy and regulatory environment. For SENTINEL, this knowledge is critical since it has impacted both the formulation and the long-term sustainability of our business model.

We shall begin our market definition approach with a distinction. In part due to the perceived lack of international consensus on basic market definition approaches in these domains, IT or cybersecurity and data privacy / personal data protection can be approached as distinct markets. However, after making the necessary separations below we are going to treat them as unified for the needs of this report, since most data sources do not take the overlaps into account.

Cybersecurity (CS) products and solutions address specific vulnerabilities or groups of threats which may arise from both external and internal malicious actors, whose capabilities are lately improving at a greater pace than SMEs' cyber defence capabilities. As companies increasingly adopt digital business models, the way they conduct business is therefore radically transformed. However, in most situations, they lack the specialists and in-house skills to secure client and transaction data, as stated in the basic SENTINEL premise. CS offerings include on-premises and Cloud-deployed software for endpoint protection (e.g., antivirus and anti-malware), security event management, Identity & Access Management systems (IAM), backup and business continuity, IDS/IPS/WAFs, application lifecycle security management, and similar products and solutions. Cyber awareness, education and training offerings are also usually positioned within this market.

From a **data privacy and personal data protection (PDP)** perspective, the market currently proposes offerings in response to increased data breaches and data leaks which allow attackers to exploit personal (sensitive or otherwise critical) information for fraud, espionage, sabotage or ransom. In Europe, the predominant data privacy regulation is the GDPR which, since coming into force in 2018, has made a considerable attempt to adapt with new technologies such as data protection and privacy-enhancing technologies, supporting, for example, the data minimisation, purpose and storage limitation and of course the appropriate data security principles and a host of other organisational and technical measures which can be supported by relevant commercial offerings. PDP offerings include on-premises and Cloud-deployed software to address specific confidentiality requirements for added privacy and protection of personal data or to address the need for control and ownership/stewardship of such data. These can be offered in the form of software for data-level encryption for anonymisation and pseudonymisation, data loss prevention software (to protect from both internal and external data leaks), record-keeping & auditing management, privacy notices and consent management and, of course, unified solutions to address data governance, risk management, DPIA audits and GDPR compliance holistically.

Another key consideration for SENTINEL is the need to specifically target SMEs and particularly small and micro businesses, initially in Europe. Market definition for these segments presents some challenges since there are no established data identifying and assessing the market

segmented per organisation size or structure. Most of the data available refer to the market as segmented in verticals. Nevertheless, it is worthy to note that, according to Mordor Intelligence [1], the European CS market size is currently around USD 57 Bn and expected to grow above USD 95 Bn by 2029 at an average CAGR (2024-2029) of ~11% (see also Section 3.2).

Having defined the two constituents of the market, in terms of the nature of the offered products and solutions, we also need to address a few additional key market characteristics, which will strengthen our understanding of the domain. These are:

- A more detailed discussion of the market outlook by industry type and geographical area (EU countries) which allows us to establish the overall status and market outlook for the region (to be tackled in Section 3.2)
- A further segmentation of the CS & PDP market (presented in Section 3.3)
  - Horizontal: A more detailed breakdown of the solutions offered by type and issue(s) addressed
  - Vertical: A study of the market verticals (segments)
- A horizontal analysis of competition (detailed in Section 4), including:
  - The positioning of GDPR/PDP, CS and training market players as active in ICT in general or specifically in the domains of GDPR/PDP, CS and training (i.e., where most of their revenue is associated with the production and sales of GDPR/PDP, CS and training solutions) the providers whose offerings are specifically addressing the needs and capabilities of SMEs and
  - End-to-end GDPR/PDP, CS and training solution providers whose offerings combine hardware, software and services.
- An overview of the overarching legal, policy and regulatory environment (tackled in the PEST and SWOT analysis)

3.2 Cybersecurity & Data Protection market outlook

In this section, we examine the major trends and drivers of the **cybersecurity market**, presenting its potential, accompanied by the European cybersecurity market outlook. We continue with the **data protection (GDPR compliance) market** at the global and European level, concluding the spending potential of SMEs in Europe.

3.2.1 Global cybersecurity market

According to market analysts, the global cybersecurity market size is projected to grow from USD 190.4 Bn in 2023 [2] to USD 298.5 Bn by 2028, recording a Compound Annual Growth Rate (CAGR) of 9.4% from 2023 to 2028. The market's growth can be attributed to the increasing awareness and rising investments in cybersecurity infrastructure across global organizations operating across verticals.

Based on another analysis [3], the global cybersecurity market is projected to grow from USD 172.32 Bn in 2023 to USD 424.96 Bn in 2030 at a CAGR of 13.8% during the 2023-2030 period. The global cybersecurity market size was USD 153.7 Bn in 2022 and the global impact of COVID-19 has been unique and staggering, with cybersecurity observing a slight negative impact on demand across all regions amid the pandemic.

The market growth is attributed to the growing need for strict compliance with regulatory requirements and increasing instances and complexities of security breaches due to insider and outsider threats. Cyber attackers are impersonating healthcare organizations and other government entities to gain access to systems and sensitive information. This factor is expected to drive the cybersecurity market.

The market is mainly driven by the emerging online e-commerce platforms and the advent of core technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), Cloud security, and others. Key players are focusing on developing internet security solutions based on AI platforms.

Rising Number of E-commerce Platforms. The rising number of e-commerce platforms and advancements in technologies such as artificial intelligence, Cloud, and blockchain has augmented Internet security solutions in a connected network infrastructure. Additionally, e-commerce companies are focused on adopting network security solutions in their IT and electronic security systems. For instance, in September 2020, Askul Corp. adopted the advanced network security solution Shadankun, developed by Cybersecurity Cloud, Inc.[1], in their business unit to secure their assets from cyber threats. This market trend is enforced by the increasing utilization of online transactions during the corona crisis. Based on PayPal's 2020 analysis [4] of transaction data from approximately 150000 SMEs in Europe, digital SMEs saw 50% (year-over-year) YoY growth despite a 15% YoY decline in GDP for the euro area during the same period.

Increasing demand for the cybersecurity mesh. The cybersecurity mesh is a modern conceptual approach to security architectures. It enables distributed enterprises to deploy and extend security where it is most needed. It is a decentralized concept that aims at protecting the identity of users or computers and it is one of the most rapidly growing strategies today. The aim is to limit access to organizations' network to approved users (or systems), whether on-premises or in the Cloud. In theory, the cybersecurity mesh helps IT experts manage protection from each access point, therefore preventing attackers from gaining access to the system without securing a single 'perimeter'.

The concept of cybersecurity mesh recognizes that networks have no physical boundaries. Organizations need to build a security perimeter around each individual user, allowing them to securely access assets from any location and device. In this model, policy enforcement would be performed through a Cloud service for assets rather than devices. The cybersecurity mesh involves designing and implementing IT security infrastructures that do not focus on building a single 'perimeter' around all devices or nodes but on establishing smaller, individual perimeters around each access point. For instance, in June 2023, Cisco introduced Secure Access, a new Security Service Edge (SSE) solution designed to enhance hybrid work by providing a single way for users to access all resources securely directing traffic across various locations, devices, and applications.

Low cybersecurity budget and high installation cost. The budget for cybersecurity in emerging start-ups is insufficient to implement Next-Generation Firewalls (NGFWs) and Advanced Threat Protection (ATP) solutions. The lack of investments and limited funding are key factors that are projected to restrict the adoption of cybersecurity solutions among small businesses. Severely restricted budgets lead to a dearth of proper IT security infrastructure,

[1] https://www.csCloud.co.jp/en/news/press/20200909616/

resulting in slow adoption of new technologies and enterprise security solutions. Small enterprises are additionally burdened with the proper management of the budget for various operations and for business continuity.

Adoption of IoT security to increase demand in the cybersecurity market. As enterprises across verticals adopt IoT devices to improve operational efficiency and enhance communication, IoT traffic is expected to rise in the coming years. The growing adoption of these IoT devices has widened the scope of attacks for cybercriminals. A cybersecurity model approach is expected to be adopted by organizations dealing with critical business and personal information in the coming years as it offers security professionals greater visibility in terms of users accessing networks from various locations, accessed applications, and the exact time of access. A single IoT device is capable of making thousands of queries every day, and users in organizations have access to multiple devices connected within or outside networks. The huge volume of requests can sometimes prevent data security professionals from entering all the requests in Security Information and Event Management (SIEM) systems [30] that can further block network-level visibility. To address such visibility challenges, enterprises are shifting toward cybersecurity solutions that inspect all the traffic within internal and external networks and detect malicious Domain Name System (DNS) queries. For example, In November 2023, IBM introduced a new product called QRadar SIEM, which is a Cloud-native SIEM system designed for hybrid Cloud environments [31], integrating advanced AI capabilities for threat detection and response, targeting the reduction of noise and improvement of alert quality.

Rapid Adoption of Security Solutions Across Healthcare and Government Sector to Boost Demand. The COVID-19 epidemic severely affected the behaviour of consumers and providers. The closure of manufacturing units, job crunches, lack of resources, data breaches, and weakened supply chains have negatively affected business growth. The pandemic impacted small businesses and start-ups worldwide especially in terms of demand for cybersecurity solutions and services. Exceptionally, the demand for cybersecurity solutions in healthcare, manufacturing, and government has grown exponentially during the pandemic. Key players in the market have focused on launching solutions to secure industrial operations against severe cyberattacks. For instance, in December 2020, IBM Corporation launched IBM Security X-Force, a threat intelligence task force to detect cyber-attacks[2]. The company also launched the Global Phishing Campaign across six countries.

Increasing Demand for Services leads to the CS market growth. Based on the component, the market is divided into solutions and services. The solutions area includes network security, endpoint security, Cloud application security, internet security, and secure web gateway. End-point security hardware, software, and access control solutions are being more widely employed in industries including IT and telecom, financial institutions, and others, boosting the segment's growth. For instance, in December 2023, IBM Consulting and Palo Alto Networks expanded their strategic partnership to enhance enterprise security, focusing on AI-driven security operations and Cloud transformation in order to strengthen end-to-end security postures for clients, addressing the accelerating threats in cybersecurity. The service category is expected to grow at the quickest CAGR over the projected period, owing to rising demand for consultancy, upgrading, and maintenance services by large and medium businesses.

[2] https://www.executivegov.com/2020/02/ibm-releases-x-force-threat-intelligence-index-2020-to-outline-cyber-vulnerabilities-wendi-whitmore-quoted/

Market Growth to be Driven by Growing Popularity of Cybersecurity Solutions with Improved Storage Capability. Based on deployment type, the market may be categorised into the Cloud and on-premises segments. The Cloud segment is expected to hold the highest CAGR during the forecast period. The growth is owing to the increasing demand for applications to store and secure data with enhanced security techniques. Also, players in the market are developing advanced Cloud-based security solutions by partnering and collaborating with other key players. For instance, in December 2019, Fortinet, Inc. completed a partnership with Google LLC to integrate its Cloud security portfolio with Google's Cloud Platform[3]. This allows the customer to shift to the Cloud platform for advanced security for their workloads. The on-premises segment is expected to grow at a considerable growth rate owing to the rising demand for managed security services.

Increasing Adoption of Network Security Solutions by SMEs to Lead to Market Dominance. Based on enterprise size, the marketplace is divided into SMEs and large enterprises. The SMEs are projected to grow at the highest CAGR. This growth is owing to the increasing demand for end-point security solutions across various e-commerce start-ups, including retail and financial sectors. The large enterprise is predicted to showcase considerable growth due to increasing demand for oud application security services.

BFSI Industry (Banking, Financial Services, and Insurance) drives the demand for Security and Digital Privacy Systems. Based on industry, the market is segmented into BFSI, IT and telecommunications, retail, government, manufacturing, travel and transportation, healthcare, energy and utilities, and others. Among all the industries, BFSI is expected to rise with a significant compound annual growth rate during the estimated period. This growth is due to the increasing demand for robust security and digital privacy systems across financial, insurance, and banking institutes. Cloud application security solutions help banks, insurance, and financial organizations secure extremely confidential data incorporated with real-time intelligence against insistent cyber-attacks. The healthcare segment is expected to experience considerable growth during the forecast period. Across the healthcare industry, internet security solutions aid in providing data protection for customer health care records. For instance, in October 2018, IBM Corporation acquired Red Hat, Inc.[4] With this acquisition, IBM Corporation developed and catered to security solutions across a wide range of industries worldwide.

The large enterprises segment is expected to support a larger market. Large enterprises account for a higher market share in terms of revenue in the global cybersecurity market. Large enterprises are reshaping their security policies and architecture to incorporate cybersecurity. Large organizations adopt cybersecurity to safeguard network, endpoints, datacentres, devices, users and applications from unauthorized usage and malicious attacks. Key players such as IBM, Oracle, Fortinet, Microsoft, and Trend Micro, along with several startups in the region are offering enhanced cybersecurity software solutions & services to cater to the needs of customers.

[3] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2019/fortinet-tightens-partnership-with-google-Cloud-provide-advanced-Cloud-security-and-accelerate-Cloud-on-ramp
[4] https://newsroom.ibm.com/2018-10-28-IBM-To-Acquire-Red-Hat-Completely-Changing-The-Cloud-Landscape-And-Becoming-Worlds-1-Hybrid-Cloud-Provider

3.2.2 European cybersecurity market

Europe is making cybersecurity a **high priority** and increasing relevant budgets accordingly. As the demand for robust Banking, Financial, Insurance (BFSI) and Defence services increases, the market for cybersecurity is expected to grow accordingly to keep up.

The Europe Cybersecurity Market is projected to reach USD 103.51 Bn in 2028 [5] from USD 49.72 Bn in 2022, growing at a CAGR of 13% during 2022-2028.

As the internet gets cheaper, faster, and more widely available than ever before, the connected devices, computers, and wearables cybersecurity will continue to grow in line with data breaches, malware, and phishing.

According to Statista [6], the outlook of European Cybersecurity market is as follows:

- It is projected to reach a size of USD 45.00 Bn in 2024.
- Security Services dominate the market with a projected market volume of USD 23.57 Bn in 2024.
- Revenue is expected to show an annual growth rate (CAGR 2024-2028) of 10.21%, resulting in a market size of USD 66.38 Bn by 2028.
- The average spend per employee in the Cybersecurity market is projected to reach USD 111.90 in 2024.
- In global comparison, most revenue will be generated in the United States (USD 78,310 Mn in 2024).

In this report, the market is segmented in Cyber Solutions and Security Services. The projection of each segment and the total revenues produced from the cybersecurity market in Europe is summarized in Figure 1.

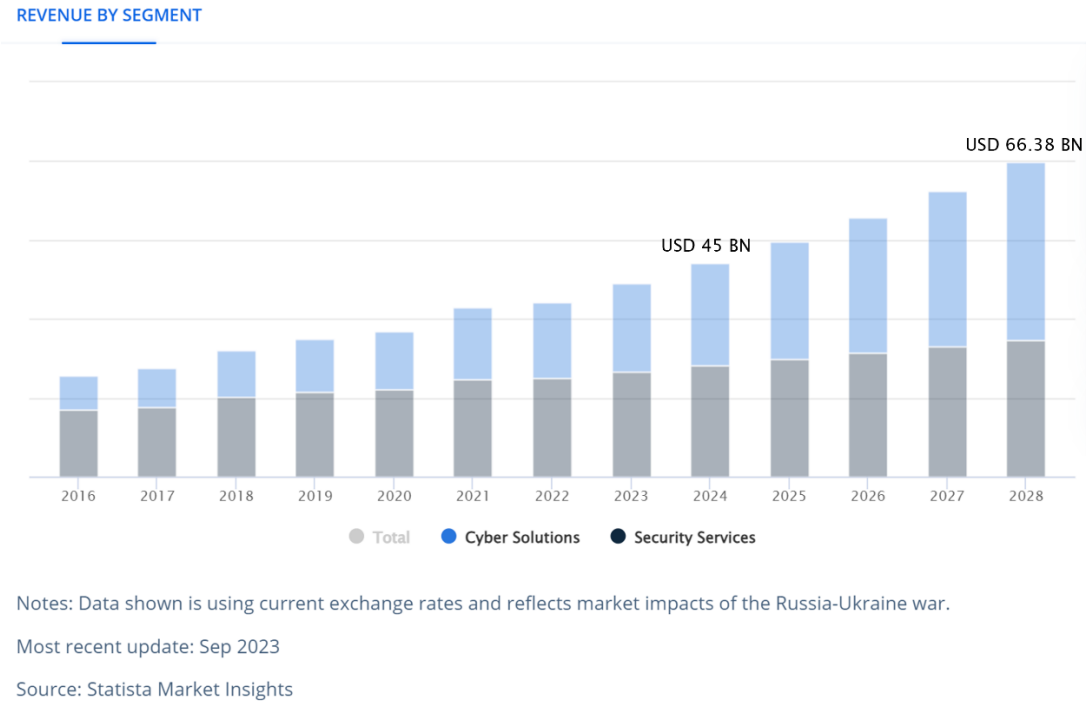

Figure 1. EU Cybersecurity revenue by Segment [6]

3.2.3 Global market for GDPR services

The global market for GDPR Services estimated at USD2.4 Bn in 2023, is projected to reach a revised size of USD 7.4 Bn by 2030, growing at a CAGR of 14.9% over the period 2023-2030 [7].

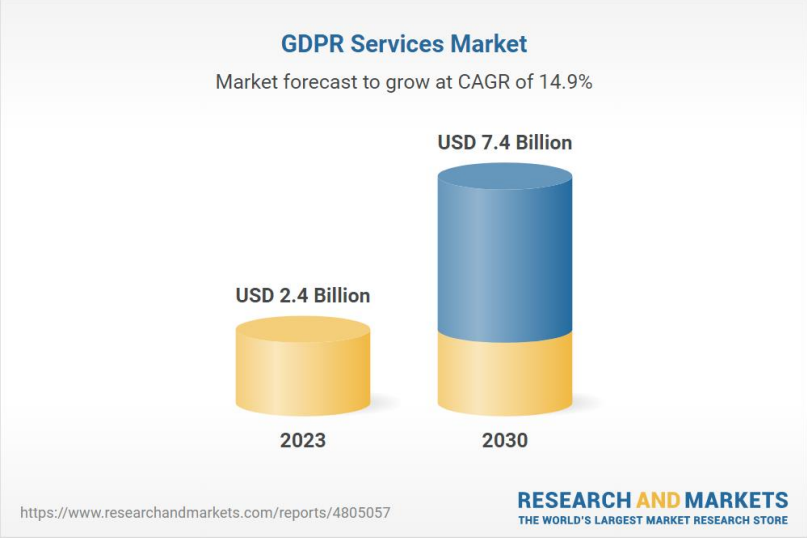

Figure 2. Global Market for GDPR Services [7]

The GDPR Services market in the U.S. is estimated at USD 499.9 Mn in 2023. China, the world's second largest economy, is forecast to reach a projected market size of USD 393.6 Mn by the year 2030 trailing a CAGR of 14.8% over the analysis period 2023 to 2030. Among the other

noteworthy geographic markets are Japan and Canada, each forecast to grow at 13% and 13.8% respectively over the 2023-2030 period. Within Europe, Germany is forecast to grow at approximately 15.6% CAGR.

According to Mordor Intelligence [8], the GDPR Services Market size is estimated at USD 3.33 Bn in 2024, and is expected to reach USD 11.30 Bn by 2029, growing at a CAGR of 27.66% during the forecast period (2024-2029).

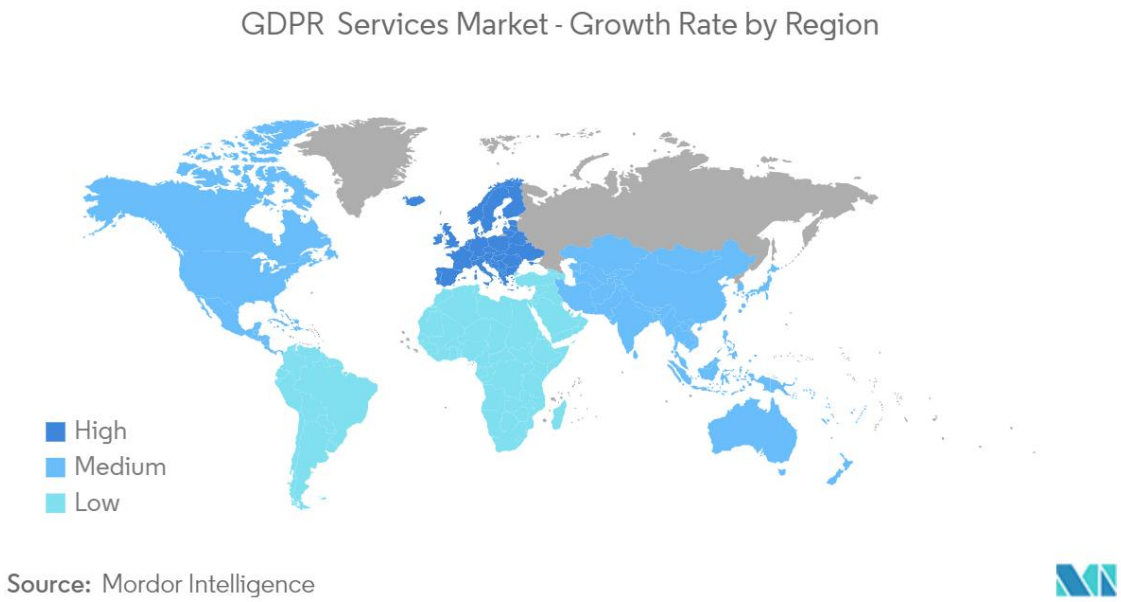

Figure 3. GDPR Services Market growth by region [8]

Because of the increased demand for characteristics such as privacy, security, authenticity, legality, trust, universality, and scalability in organizational operations and quality monitoring, the GDPR services industry has a lot of room to develop. GDPR services are projected to witness a significant increase in demand as concerns about data privacy and security develop. In recent years, the number of reported cybersecurity incidents has increased considerably, underscoring the importance of data security and protection initiatives.

The growing prevalence of Cloud computing around the world is expected to drive up demand for GDPR services, given the Cloud's vulnerability to cyberattacks is considerable. Small and medium businesses (SMEs) are projected to be financially impacted when registering for GDPR services because large corporations have the resources to invest in their IT and legal teams for ultimate compliance, whereas SMEs do not.

3.2.4 European market of GDPR compliance

This statistic (Figure 4) shows the estimated EU market value of services for GDPR compliance for 2023 with a forecast to 2030. By 2030, the market value of businesses offering services of compliance to GDPR is expected to reach ~ USD 4.2 Bn [9].

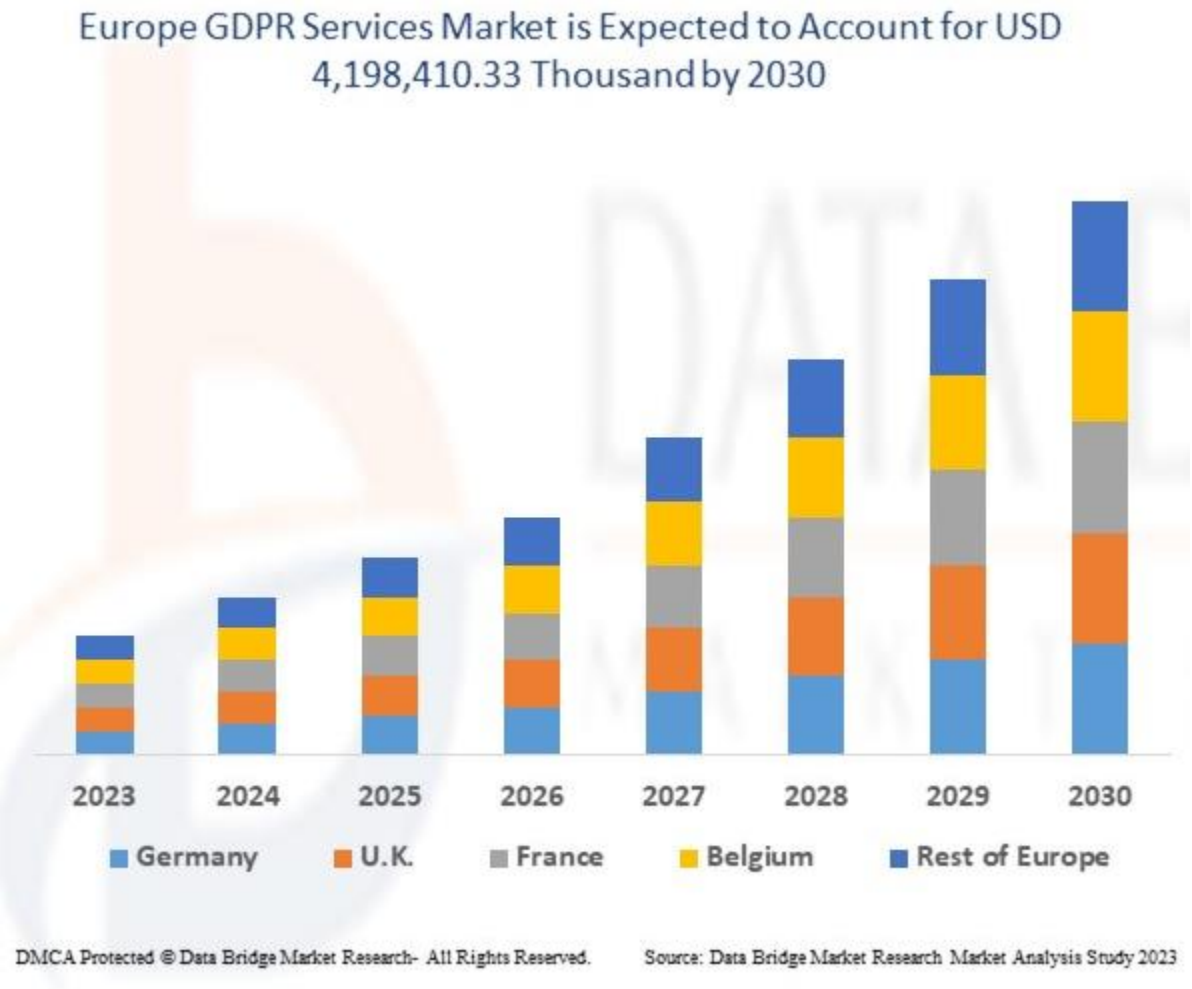

Figure 4. Market value of services for GDPR compliance in Europe [9]

Europe is anticipated to witness a significant share for GDPR services due to the high acceptance of the GDPR in the region. The rising generation of enormous amounts of data is bound to increase the demand for GDPR services (especially in the retail and healthcare sector), which – in turn – is expected to drive Europe's market growth. Companies rely on this data to make informed business decisions using a single and trusted source of information about products and customers.

Many different domains have already started facing GDPR compliance issues in Europe (e.g. personal data used in IoT-connected cars can be leveraged to track people, energy consumption data from smart meters can be used to extract consumer patterns, etc.). European data protection authorities have received a very high number of data breach notifications since the EU's new privacy law went into full effect, while regulators in many European countries have imposed GDPR-related fines in the order of hundreds of millions. More specifically, in the 2023 GDPR Enforcement Tracker Report [32] it is reported that:

- Up to March 2023, a total number of 1576 fines (+545 in comparison to the 2022 report) were issued and recorded in the Enforcement Tracker (the database also includes cases with limited / no detailed information, leading to an overall total of 1,672 cases)
- The total sum of fines amounts to around EUR 2.77 Bn (+1.19 Bn in comparison to the 2022 report). In the whole reporting period 2018-2023, the average fine was around EUR 1.8 Mn across all countries. The higher average figures in comparison are mainly due to some massive fines against “Big Tech” imposed in 2021/2022.
- Leading the list of types of violations regarding the number of fines and average amount are “insufficient legal basis for data processing” (495 fines, average EUR 0.9 Mn) and “non-compliance with general data processing principles” (Art. 5 GDPR, 381 fines, average EUR 4.5 Mn). Next on the list are “insufficient technical and organisational measures to ensure information security” (279 fines, average EUR 1.3 Mn) and “insufficient fulfilment of data subjects' rights” (150 fines, average EUR 1.5 Mn).

However, these numbers reflect only the fines that are widely visible and reported in the Enforcement Tracker. There are still a large number of cases not reported or made public. Consequently, for the organizations that deploy connected solutions (e.g. IoT-enabled applications, smart cars, smart meters, etc.), it has become pivotal to secure the protection of end users’ data. This is expected to drive up the demand for data protection compliance services and providers.

3.2.5 European SMEs’ GDPR compliance spending

Recent surveys on GDPR compliance and associated expenditure among European SMEs [33][34] report that about 15% of employees working in SMEs of France, UK, Spain, and Ireland believed their enterprises did not describe their data processing activities in clear and plain language to individuals. Another 10% stated their companies did not obtain consent or determined a lawful basis before using personal data (Figure 5). However, a large number of European SMEs surveyed reported to have spent from EUR 1,000 up to EUR 50,000 (Figure 6).

Consequently, although companies still have obligations to fulfil regarding GDPR compliance, they are willing to invest in relevant activities. Although every organisation will have its own challenges, a strong plan of action should begin with a DPIA (Data Protection Impact Assessment), a process that helps identify, assess and manage the risks associated with an organisation’s data processing practices. Similarly, risk assessments are crucial for helping identify the personal data an organisation processes, locating that information and identifying the associated risks. This results in a list of measures it can take to mitigate or eradicate threats, helping identify the most appropriate risk management strategies.

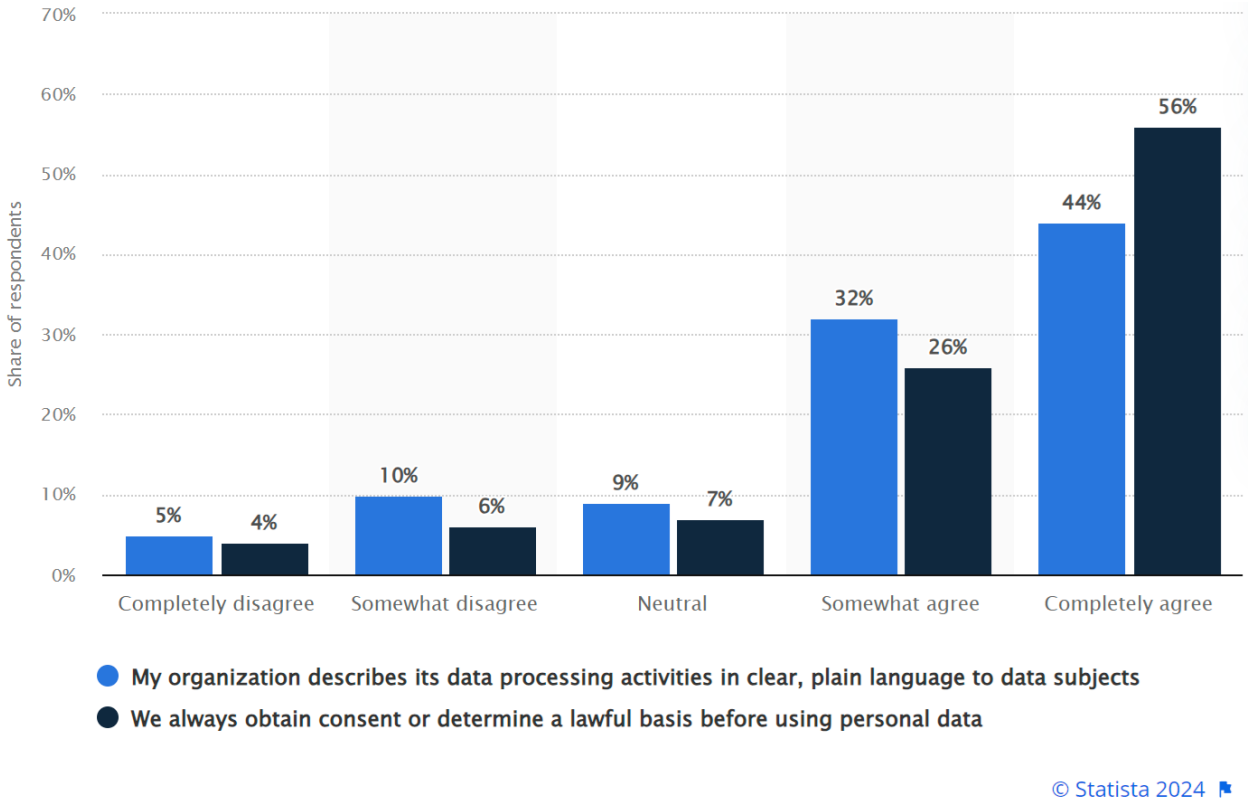

Figure 5. Share of European SMEs compliant with the GDPR in 2019 [33]

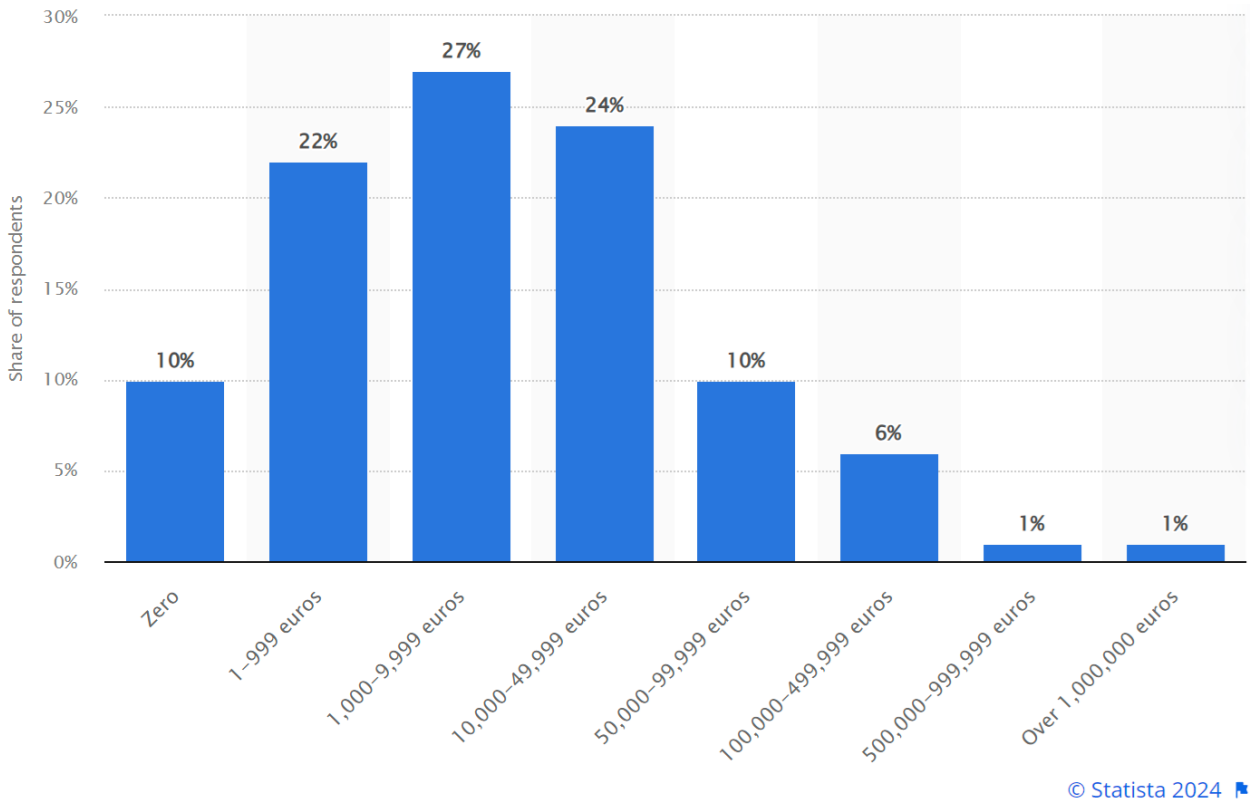

Figure 6. Share of European SMEs spending on compliance with the GDPR in 2019 [34][35]

3.3 SMEs profiling and categorisation

SMEs currently dominate the international business landscape and constitute the backbone of the EU economy, promoting competitiveness and investments of the Digital Single Market (DSM).

3.3.1 SMEs profiling

SMEs come in three sizes-bands:

(a) micro-sized enterprises which employ between 0 and 9 people,
(b) small businesses that employ between 10 and 49 people, and
(c) medium-sized businesses that have between 50 and 249 employees.

Based on the latest estimations [10][22], there were approximately 24.4 million SMEs in the EU in 2023, accounting for around 99.8% of all enterprises in the EU-27 Non-Financial Business Sector (NFBS) (Figure 7). The vast majority of these enterprises (around 94%) were micro-sized firms. Furthermore, almost 52% of the total value added produced by the EU27 NFBS and more than 64% of total EU-27 NFBS employment was generated by EU-27 SMEs in 2023 (Figure 8).

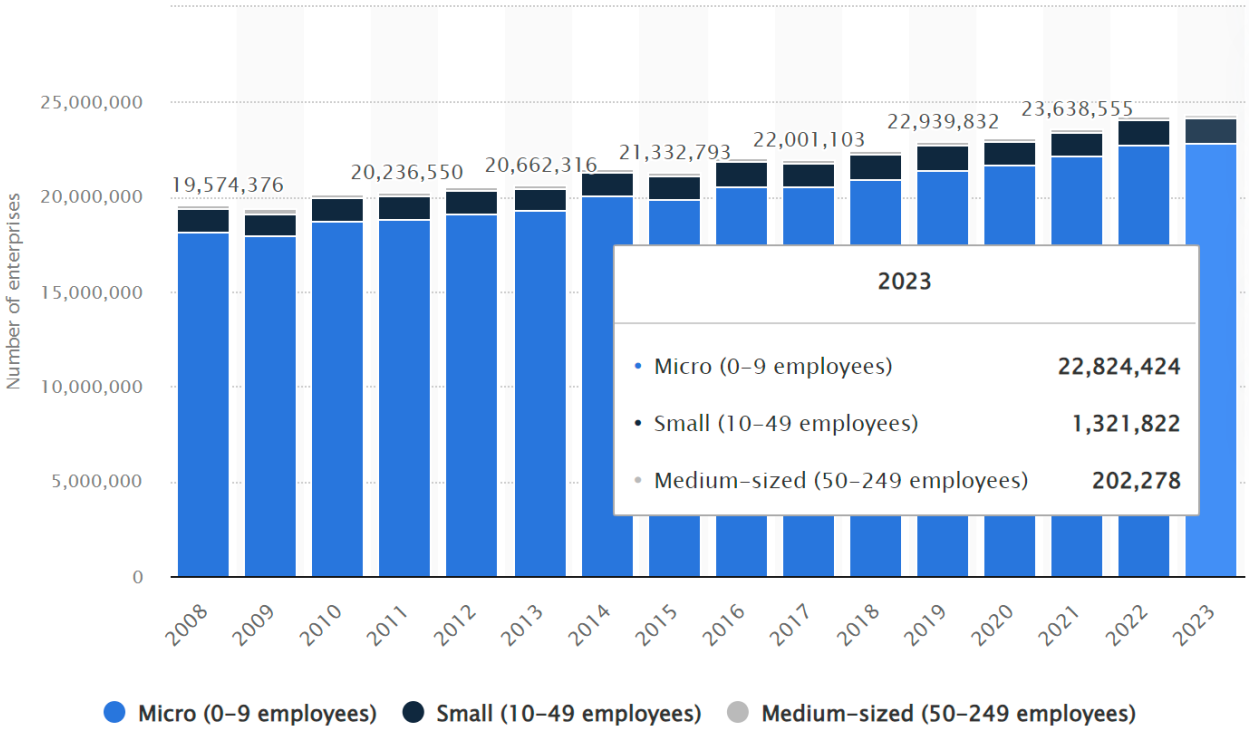

Figure 7. Number of SMEs in the EU from 2008 to 2023 [22]

Class size	Number of enterprises		Number of persons employed		Value added	
	Number	Share	Number	Share	**Billion €**	Share
Micro	22 744 173	93,5%	38 790 351	29,4%	1419,4	18,6%
Small	1 332 200	5,5%	25 602 334	19,4%	1259,8	16,5%
Medium-sized	204 786	0,8%	20 493 722	15,5%	1266,5	16,6%
SMEs	24 281 159	99,8%	84 886 407	64,4%	3945,8	51,8%
Large	43 112	0,2%	46 918 978	35,6%	3673,8	48,2%
Total	24 324 271	100,0%	131 805 385	100,0%	7619,6	100,0%

Figure 8. European SMEs Profiling [10]

According to the same annual report on European SMEs for 2022/2023 [10], the EU-27 Member States experienced a large economic downturn (in terms of GDP) in 2020 reflecting the Covid-19 pandemic effects, falling by 6.3% in 2020 after having grown by 1.6% in 2019. Despite the end of the pandemic, new challenges forced a lesser recovery in 2022 compared to initial estimations. Historically high inflation and consequences originating from the Russian-Ukrainian war, led to reduced growth rates (2022 EU-27 Gross Domestic Product (GDP) increased by 3.5% after having grown by 5.3% in 2021).

EU-27 SMEs and more specifically micro SMEs, had a positive reaction to the end of the pandemic in 2021. Moreover, EU-27 SMEs rebounded even further in 2022, with their value

added in the NFBS growing by 6.7% and their employment increasing by 2.4%. This happened almost in every industry, with the largest increases recorded in “mining and quarrying” (23.0%), “water supply” (20.0%) and “Electricity, gas, steam and air conditioning supply” (18.1%), while employment increased in almost all industries as well, with the largest increases noted in “real estate activities” (4.4%) and “information and communication” (3.6%). The number of SMEs also increased in 2022 in every industry, partly due to the considerable financial assistance provided by governments to SMEs, in order to revert the effects of COVID-19 during the years before [10].

For 2023, micro-SMEs value added is forecast to rise by 5.6%, while a smaller increase of 0.5% is expected for SME employment. Overall, added value and employment for all EU-27 SMEs are predicted to be higher compared to their respective 2019 levels, by 17.1% and 0.2%, respectively [10].

SMEs play an important role in the ‘non-financial business economy’ of the EU-27. Average SME productivity, calculated as value added per person employed, was approximately EUR 21500 and the average number of employees was 3.5.

3.3.2 SMEs digital transformation

Digital technologies play a crucial role in fostering economic growth. They enhance internal business operations, facilitate the creation of products and services, including pioneering innovations, and enable businesses to extend their reach into new markets and geographical areas. In order to meet their digitalization objectives, SMEs are increasingly depending on IT networks, systems and applications, while many have an online presence, offering digital services to their customers. They do so by establishing their own IT infrastructure and/or by relying on third party services and technologies, such as those of Cloud computing services and IoT applications. Consequently, harnessing the power of digital technologies effectively often demands investments in both hardware and software, whether on-premises or in the Cloud, alongside training to leverage their capabilities fully. Additionally, access to robust broadband infrastructure is essential for SMEs to capitalize on data-driven tools.

According to Flash Eurobarometer 486 [11] 2021 survey on “SME’s, start-ups, scale-ups and entrepreneurship”, the main barriers and challenges that SMEs in Europe face when growing, transitioning to more sustainable business models and digitalization are summarized as follows:

- One third of EU-27 SMEs had adopted or was planning to adopt basic digital technologies but not advanced digital technologies, and a quarter of EU-27 SMEs had already introduced advanced digital technologies or were planning to do so.
- However, the figures for the SME population as a whole mask large differences within the different size classes of the SME population.
    - A much larger proportion of micro-SMEs than of small and medium-sized SMEs focused only on basic digital technologies and not on advanced digital technologies (36.5% of micro-SMEs versus 29.2% of small SMEs and 26.9% of medium-sized SMEs).
    - In contrast, a much smaller proportion of micro-SMEs than of small and medium-sized SMEs were of the opinion that advanced digital technologies should be introduced, or they had already been introduced (19.9% of micro-SMEs versus 29.9% of small SMEs and 37.5% of medium-sized SMEs).

- Moreover, 20.3% of micro-SMEs were of the opinion that there was no need to introduce any kind of digital technologies. In contrast, only 15.8% of small SMEs and 9.8% of medium-sized SMEs shared this opinion.

Digital tool	All SMEs	Micro SMEs	Small SMEs	Medium-sized SMEs
The SME has adopted or is planning to adopt basic digital technologies such as email or a website but not advanced digital technologies	34.5%	36.5%	29.2%	26.9%
There is a need to introduce advanced digital technologies but the SME does not have the knowledge or skills or financing to adopt them	8.0%	8.1%	7.9%	7.3%
There is a need to introduce advanced digital technologies and the SME is currently considering which of them to adopt	9.4%	8.5%	11.7%	13.7%
There is a need to introduce advanced digital technologies and the SME has already started to adopt them	22.9%	19.9%	29.9%	37.5%
The SME does not need to adopt any digital technologies	18.9%	20.3%	15.8%	9.8%
Other, none of the above, don't know, no answer	6.3%	6.7%	5.5%	4.8%
Total	100%	100%	100%	100%

Note: Responses to Q22 in the survey. Respondents could select only one of the possible responses. Overall, the Eurobarometer response sample comprised 16,365 responses. For the purpose of the analysis in this report, the following survey responses were excluded: a) 3,750 responses from survey participants located in countries outside of the EU-27; b) 633 responses from survey respondents locacted in the EU-27 with 250 or more employees; c) 116 responses from survey participants located in the EU-27 who did not provide information on the number of their employees; d) 1,225 responses from survey respondents who indicated that they had closed their business; and, e) 239 responses from survey respondents who did not report the age of their business. As result, the response sample used in the analysis of the digitalisation of SMEs comprised 10,402 responses.
Source: Flash Eurobarometer 486 survey

Figure 9. SMEs state of digitalization, source: Flash Eurobarometer 486

According to the SME survey, larger SMEs are more likely to have a strategy or an action plan to guide their digitalisation activities, with 59% of medium-sized SMEs and 49% of small SMEs reporting having such a plan, compared to only 32% of micro-SMEs.

The key digitalisation activities reported as being under consideration by SMEs with strategies or action plans to digitalise were roughly of equal importance:

- improve their internal ICT skills (77% of SMEs)
- change their use of social media (74% of SMEs)
- improve their ICT security systems (72% of SMEs)
- adopt more advanced technologies (71% of SMEs)
- introduce online marketing and/or sales (60% of SMEs).

Looking at the plans for SMEs to digitalise in the future, 41% of SMEs having participated in the SME survey reported that they had a strategy or action plan to digitalise in the future. However, this figure varied widely across SME size classes and Member States. Larger SMEs were more likely to have a strategy or action plan to digitalise, with 32% of micro-SMEs reporting that they had a strategy or action plan, while the figure was 49% for small SMEs and 59% for medium sized SMEs. Across Member States, the figure ranged from 31% of SMEs in FR to 65% of SMEs in EL.

The types of activities identified by SMEs in their strategies or action plans to digitalise were viewed as being broadly of equal importance with:

- 60% of SMEs focusing on online marketing and/or sales
- 71% of SMEs considering the adoption or more advanced technologies
- 72% of SMEs looking to improve their ICT security systems
- 74% of SMEs planning to change their use of social media
- 77% of SMEs looking to improve their internal ICT skills

A similar report from 2021 from the Organisation for Economic Co-operation and Development (OECD) [23] indicates that small businesses are falling behind in the digital transition when compared to medium-sized and large companies (Figure 10). Moreover, it highlights that the gap in digital adoption has widened even more in recent years. Additionally, there exist notable differences in the extent of digital adoption and the types of tools embraced. For instance, within knowledge-intensive industries like information and communication services, adoption rates are notably higher, with 90% of employees in SMEs having access to online-connected devices, compared to an average of 50% across all sectors. Furthermore, the significance of various digital tools varies across sectors. In the accommodation and food services sector, for instance, possessing a high-speed broadband connection, a website, and utilizing Cloud services for file storage significantly enhance value for SMEs. Conversely, in the wholesale sector, critical technologies include electronic sales, leveraging Cloud services for database hosting, and the training of Information and Communication Technology (ICT) specialists.

Despite the pandemic serving as a catalyst for digital transformation and novel business models, the OECD report highlights persistent long-term structural barriers for SMEs. These barriers include deficiencies in digital skills, limited access to finance, and inadequate infrastructure.

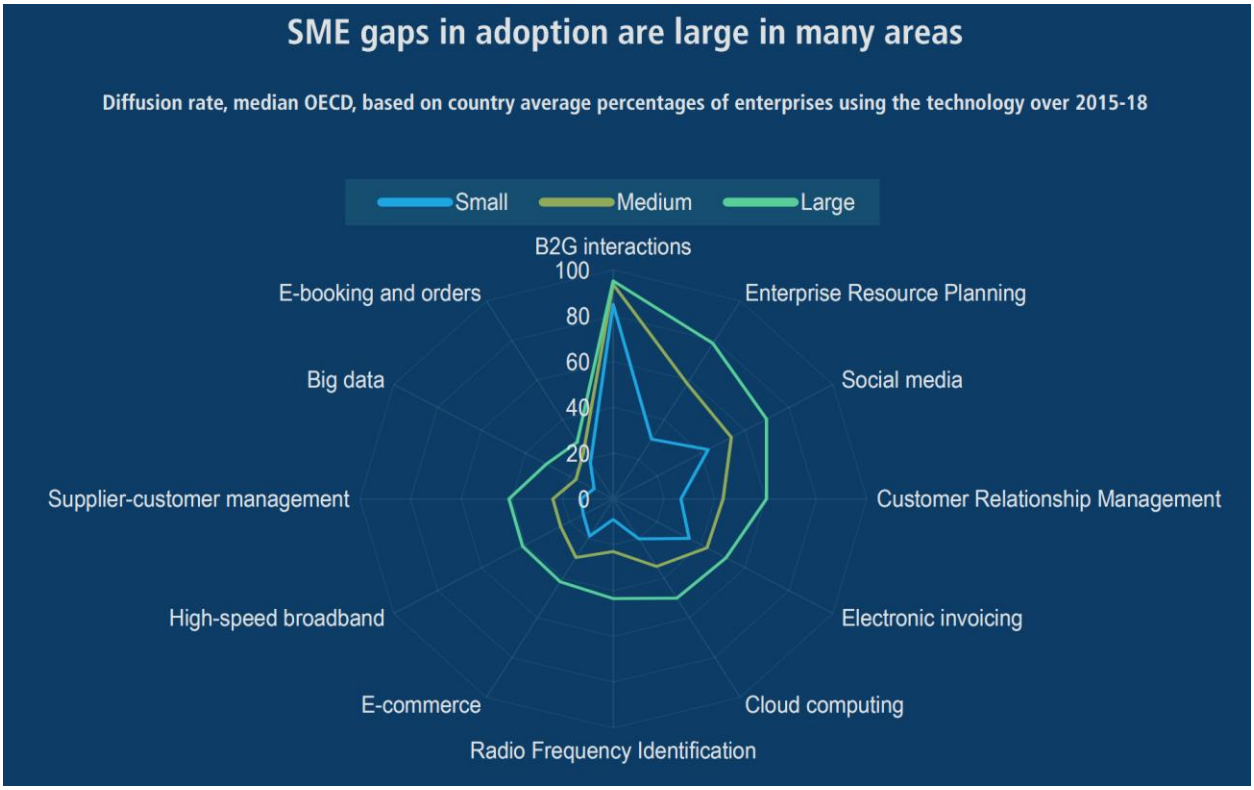

Figure 10. SME gaps in adoption of digital solutions

The European Commission's Digital Economy and Society Index (DESI) index, which gauges the digital intensity level in businesses across various areas such as e-commerce, Cloud services, and artificial intelligence (AI), indicates progress in certain countries. However, significant disparities persist, and advancements have been gradual, particularly among SMEs. For instance, in 2022 [24][25], 70% of all EU businesses reached a basic level of digital intensity (i.e., at least 4)[5]. The share for SMEs was 69%, while for large businesses it stood at 98%. Large businesses had a bigger share for very high (30%) and high digital intensity (54%) compared with only 4% of SMEs with a very high level and 27% with a high level of digital intensity. Most of the SMEs recorded low (38%) or very low (31%) digital intensity levels (Figure 11). Additionally, in 2021, only 8% of businesses in the EU used AI, 41% bought Cloud computing services and 14% were making use of big data. These figures fall considerably short of the targets set by the Digital Decade initiative [26], which aims for over 90% of European SMEs to achieve a basic level of digital engagement and for 75% of EU companies to adopt Cloud, AI, and big data technologies.

[5] 0-3: very low; 4-6: low; 7-9: high; 10-12: very high

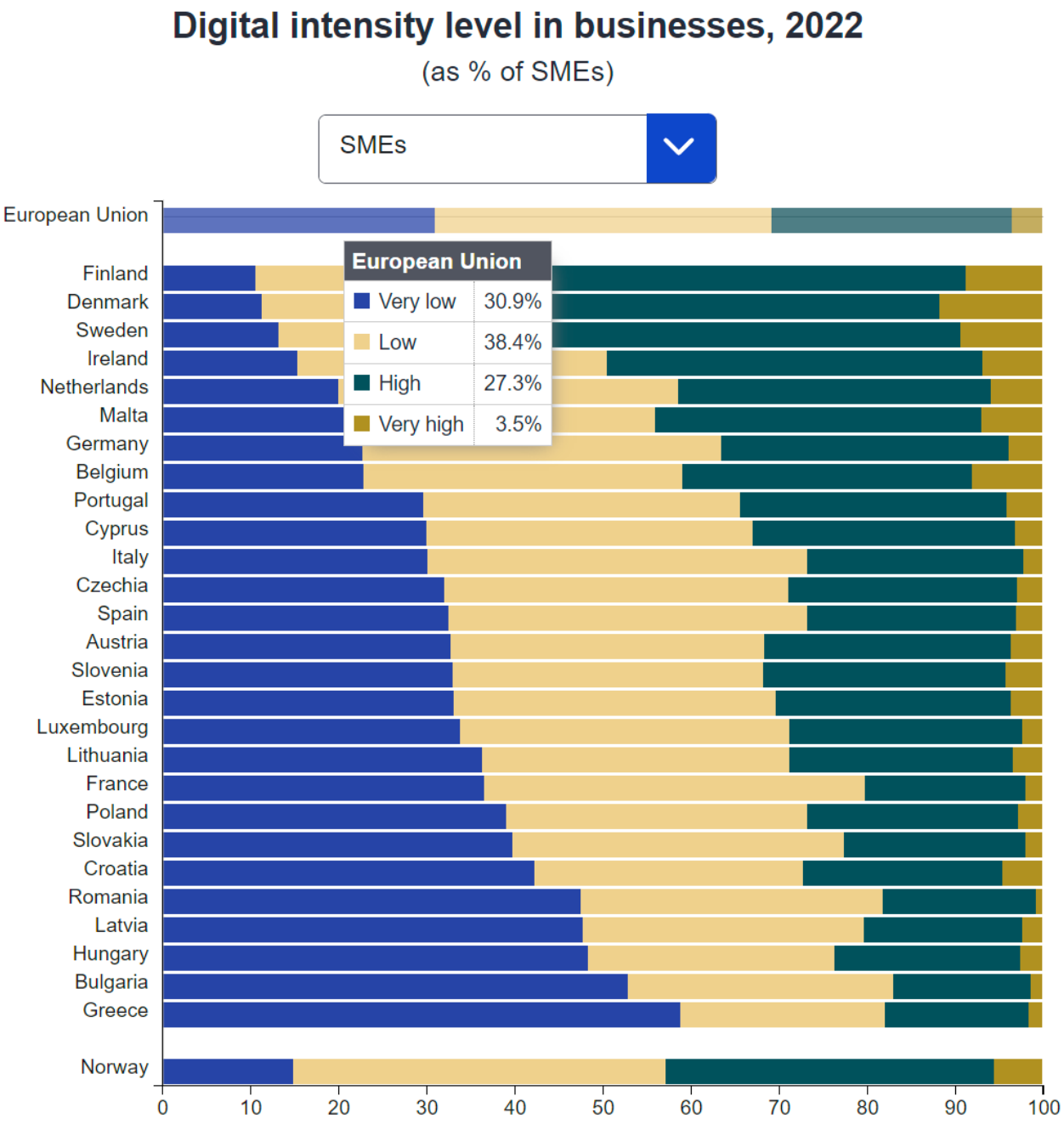

Figure 11. Digital intensity level in SMEs [24]

SMEs (especially those not directly engaged in the ICT sector) encounter several distinct hurdles that hinder their capacity to leverage the digital transition and sustain a competitive edge. These enterprises have to face **the lack of financial resources, the lack of skills including managerial skills and potential infrastructure gaps** [27]. More specifically:

- **Financial barriers**. These challenges may emerge because SMEs encounter obstacles in securing financing for digital investments that are not eligible as collateral for loans.

- **Structural barriers**. These challenges may arise due to a skills gap, preventing managers and employees from recognizing the digital solutions required and adjusting business models and processes to capitalize on potential productivity enhancements and advancements in trade, including cross-border transactions.
- **Potential infrastructure gaps**. Smaller enterprises might not be prioritized by providers for high-speed broadband installation, and they might lack the resources to invest in dedicated connections necessary for utilizing advanced technologies like big data processing and AI.

These factors play an important role in reducing the likelihood of adopting both basic and advanced digital technologies. Firms which reported uncertainty about future digital standards, internal resistance to change, regulatory obstacles or IT security issues as barriers to digitalisation are more likely to have adopted advanced digital technology. This result may be due to reverse causality whereby those firms that have adopted advanced digital technologies will encounter these barriers, but basic digital technology adopters may not necessarily be focused on (some of) these barriers.

The high volume of SMEs, as depicted by the SMEs profiling, reflects on the high volume of data that are processed by them, much of which is personal data. Personal data is defined under the EU General Data Protection Regulation (GDPR) as “any information relating to an identified or identifiable natural person (data subject)”. When processing personal data, SMEs have certain legal obligations arising from GDPR. In particular, SMEs will very often take the role of the data controller, e.g., when processing personal data of customers or staff. Sometimes they may also take the role of data processor, e.g., when providing services to customers on behalf of another company. The criticality of the personal data processing performed by an SME may vary. For example, while a retail shop will only process personal data related to purchases of goods, a medical diagnostic centre will engage in the processing of health data of its clients and a dating site will maintain detailed personal profiles of its users. One of the core obligations for data controllers and processors in GDPR is that of the security of personal data. More specifically, according to GDPR, security equally covers confidentiality, integrity and availability and should be considered following a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk).

3.3.3 SMEs cybersecurity outlook

Taking into account the increasing use of digital and/or online data processing systems, often based on Cloud services and smart IoT devices, security risks for personal data are associated today to a great extent to the security risks of the underlying IT networks and system components. ENISA’s report “Cybersecurity for SMEs” [12] analyses the ability of SMEs within the EU to cope with the cybersecurity challenges posed by the pandemic and determines best practices to mitigate those risks.

Low awareness of the threats posed to businesses by poor cybersecurity; the costs of implementing cybersecurity measures, often combined with a lack of dedicated budget; the availability of ICT cybersecurity specialists; a lack of suitable guidelines aimed at the SME sector; and low levels of support from management were among the main challenges identified during the study's interviews. The underlying issue appears to be management understanding and commitment, which drives budget/resources allocation, and successful cybersecurity practice

execution. Cybersecurity is not just a topic for IT departments to talk about; it needs to make its way into boardrooms as well.

Of the 249 European SMEs surveyed more than 85% stated that cybersecurity issues would have serious negative impacts on their business within a week of the issues happening; 57% say they would most likely become bankrupt or go out of business.

Despite this, there is a popular notion that cyber incidents mostly impact larger organizations, and that SMEs are therefore not a significant threat. Small businesses must be aware of the impact such incidents will have on their operations if they occur. Many SMEs believe that the cybersecurity measures built into the IT products they buy are adequate and that they don't require any additional security controls unless they are mandated by law.

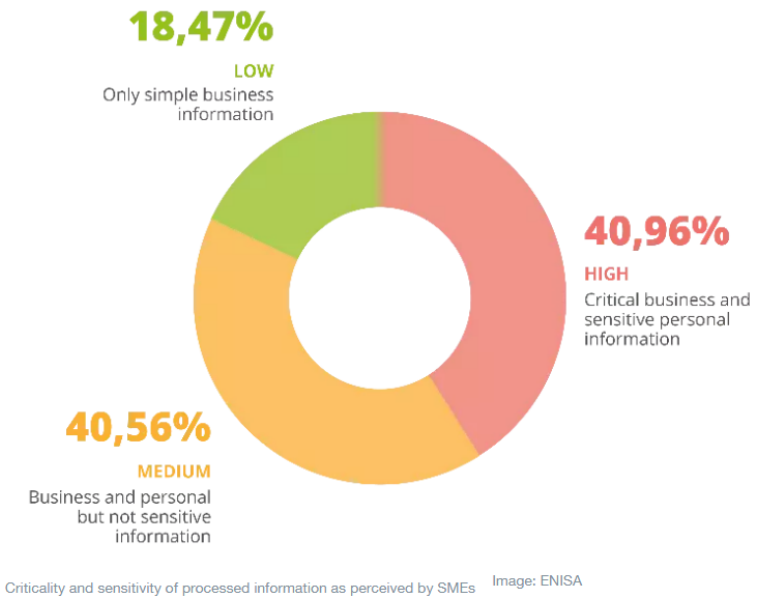

Figure 12. Criticality and sensitivity of processed information, source: ENISA

The agency's cybersecurity advice towards SMEs focuses on three crucial areas: people, processes, and technical recommendations. The aim is to strengthen resilience across the whole value chain through the application of the 12 cybersecurity principles and the report includes suggested actions that the EU Member States should consider in order to support businesses, associations, and agencies in improving their cybersecurity posture.

A similar survey entitled "Europe's SMEs in the Digital Decade 2030: building cyber-resilience, overcoming uncertainty" [28], found that while 92% of SMEs recognised the threat posed by cybercrime, only 16% of businesses felt very well prepared for a potential attack, despite the fact that 43% of firms were attacked in the previous year. Additionally, other than the lack of knowledge/skills and funds (that coincide with the results from [27]), the third most important obstacle to further investment in digital transition was "Concerns about cybersecurity risks" (Figure 13):

- 45% of SMEs that participated in the survey cited lack of knowledge/skills as a barrier to digitalisation (46% of SMEs said they had been unable to hire cybersecurity experts due to lack of qualified specialists/cost of hiring)
- 31% of SMEs mentioned lack of funds as a barrier to digitalisation
- 27% of SMEs reported cybersecurity as a barrier to digitalisation

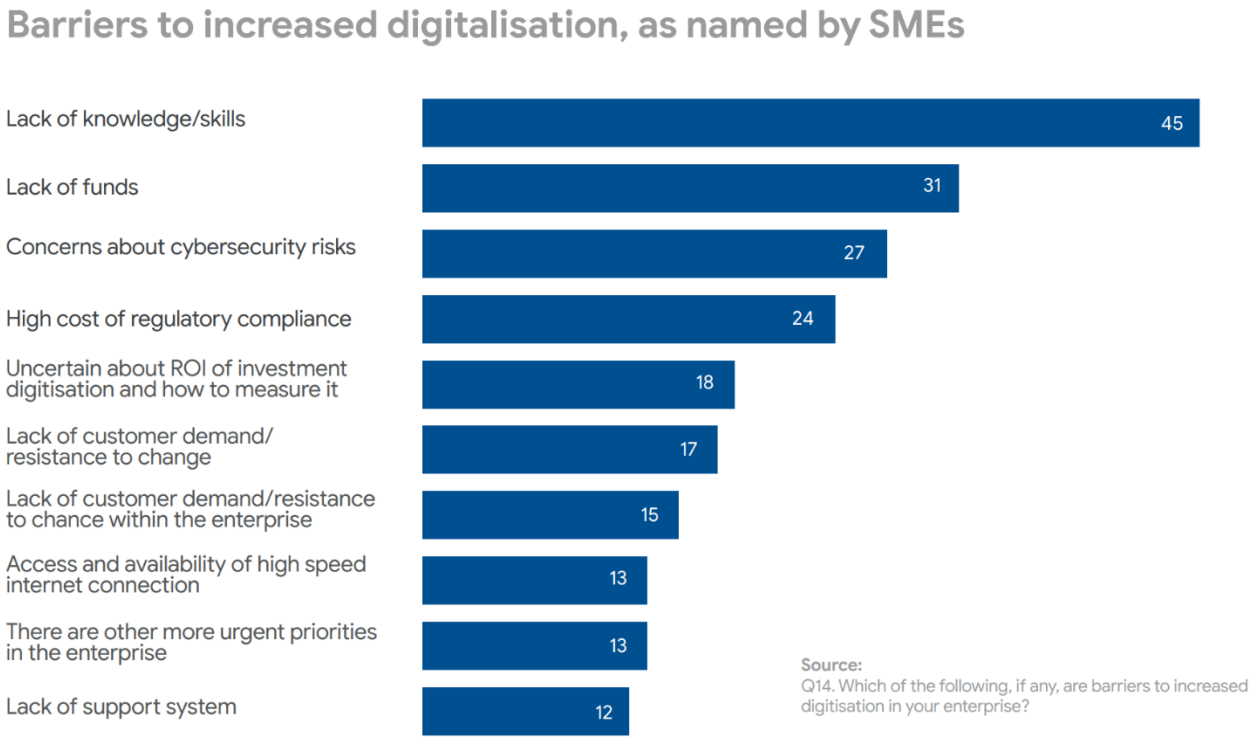

Figure 13. Barriers to increased digitalization [28]

In a nutshell, the report proposes a multi-pronged approach to tackle these barriers:

- **Training and certification programs**: SMEs find it hard to hire people with digital skills, whether that's an entry-level role or a cybersecurity expert. Tackling this requires lifelong learning and constant upskilling. This approach could ease talent shortage.
- **Performance evaluation of the financial assistance**: Multiple EU programmes and initiatives already provide support from tackling late payments to improve cash flow for SMEs to direct support through the EU Recovery and Resilience Facility (RRF) [27]. One area for further research could be to undertake a comprehensive performance evaluation of the financial assistance mechanisms across Europe.
- **Cybersecurity education/awareness/training and implementation support**: The SMEs need to be informed about the benefits of digital transition on their own terms, and supported to build their cybersecurity toolkit.

Effective cybersecurity provides SMEs with the confidence to grow, innovate and find new ways of creating value for customers. SENTINEL will support these businesses on their journey to consolidated data security and data protection compliance.

3.3.4 SMEs data protection/GDPR outlook

When the GDPR took effect in May 2018, it was largely expected that the regulation would have the most impact on large tech companies. However, a number of articles and publications (e.g., [36][37][38]) indicate that although "*GDPR has successfully met its objectives of strengthening the protection of the individual's right to personal data protection and guaranteeing the free flow of personal data within the EU*", there are still a number of challenges and areas for improvement when it comes to SMEs fully implementing the GDPR. Some of the main reasons behind non-compliance among SMEs are:

- **Knowledge:** The majority of SMEs are aware of GDPR, but don't know how to deal with.
- **Complexity:** SMEs don't understand the GDPR to its full extent and what requirements they have to fulfil in order to become compliant.
- **Expertise:** Access to professional expertise and tools is costly.
- **Relevance:** A lot of SMEs are relying on the assumption that they will go unnoticed as authorities are still mainly targeting larger companies.
- **Resistance:** In many cases, the higher management in SMEs proves reluctant to invest the necessary time and funds to investigate how they can become compliant with the GDPR,

as supported also by another GDPR readiness survey [39] and depicted in Figure 14.

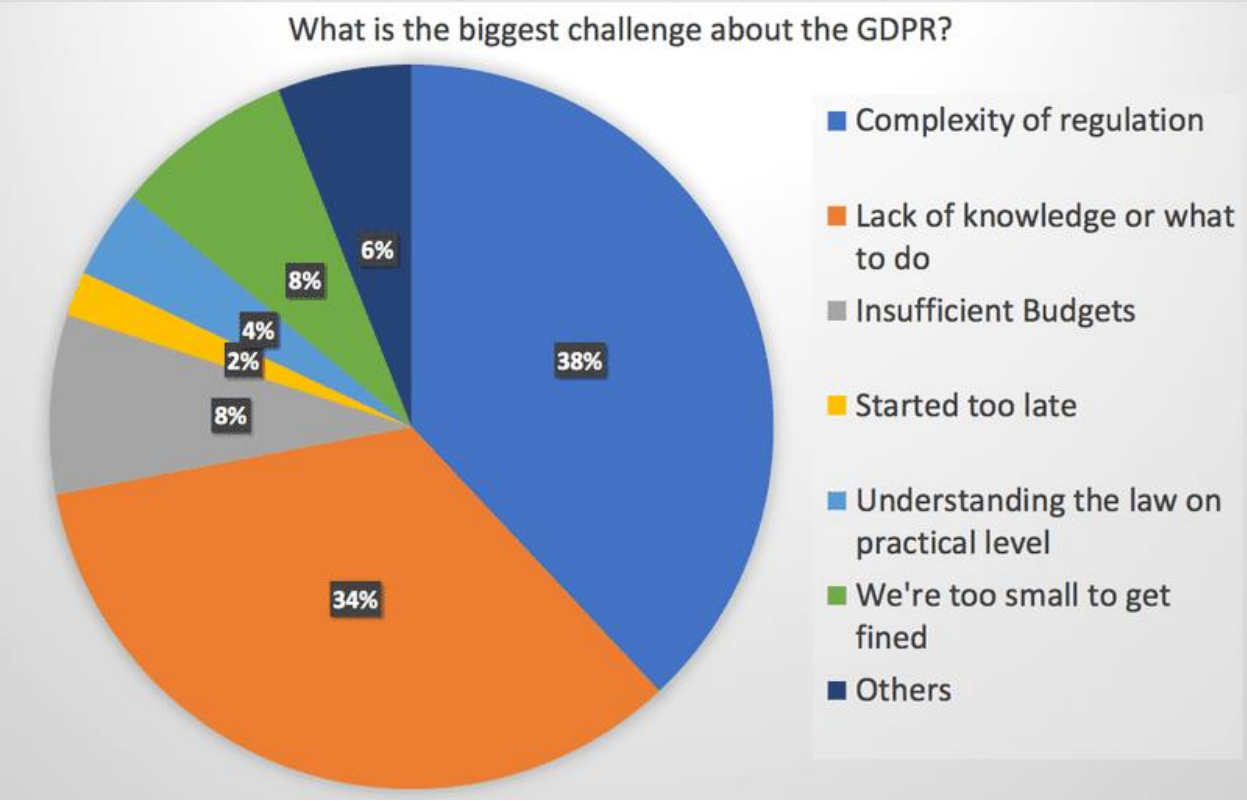

Figure 14. Biggest challenge in the GDPR [39]

Furthermore, a recent detailed survey [29] conducted a classification of challenges associated with GDPR compliance that it identified in recent studies and categorized them in four main categories as listed in Table 2 below:

Table 2. Classification of GDPR challenges

Category	Subcategories	Challenges
Technical	Technical complexity	• Redesigning systems to comply with the GDPR • Managing data, especially aggregated • Enforcement of security means • Mapping personal data
Legal	Legal compliance	• Legal documentary complexities • Legal uncertainty • Difficulty of balancing between GDPR and other legal and regulatory requirements
Organisational	Lack of expertise	• Lack of knowledge, expertise, and experience
	Cost concerns	• Monetary costs • Human costs • Expenditure of time
	Process adaptation	• Adaptation of internal processes • Establishing new procedures
	Corporate governance	• Resistance to change, culture of privacy, systems/policy change, risk management models
	Vendor management	• Ensuring compliance by third-party vendors • Relationship management • Dealing with third parties to erase private data
Regulatory	Regulation complexity	• Complexity of the GDPR Regulation • Lack of awareness and understanding of the GDPR requirements
	Insufficient government support	• Incomplete or vague guidelines and little support from authorities

Additionally, the GDPR readiness survey [39] showed that only half of the companies that they interviewed sought external help for (Figure 15) and believed to be fully compliant with (Figure 16) the GDPR, leaving them open to misinterpretations of the regulation and leading them possibly to heavy fines.

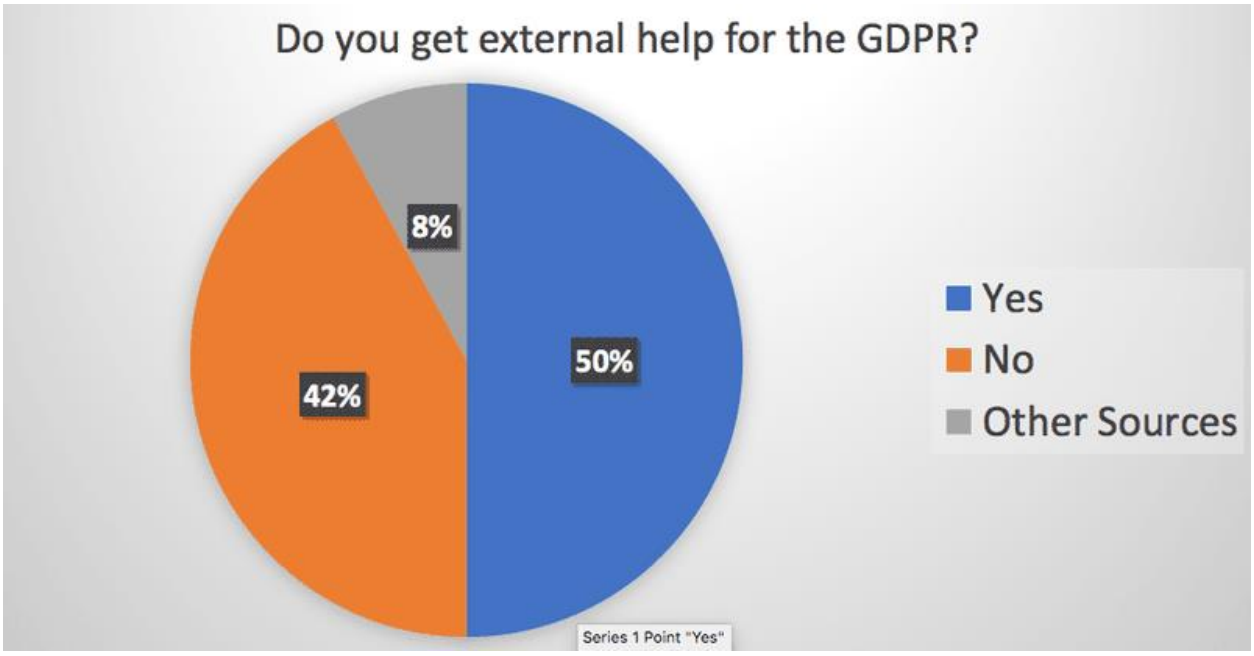

Figure 15. External vs internal help [39]

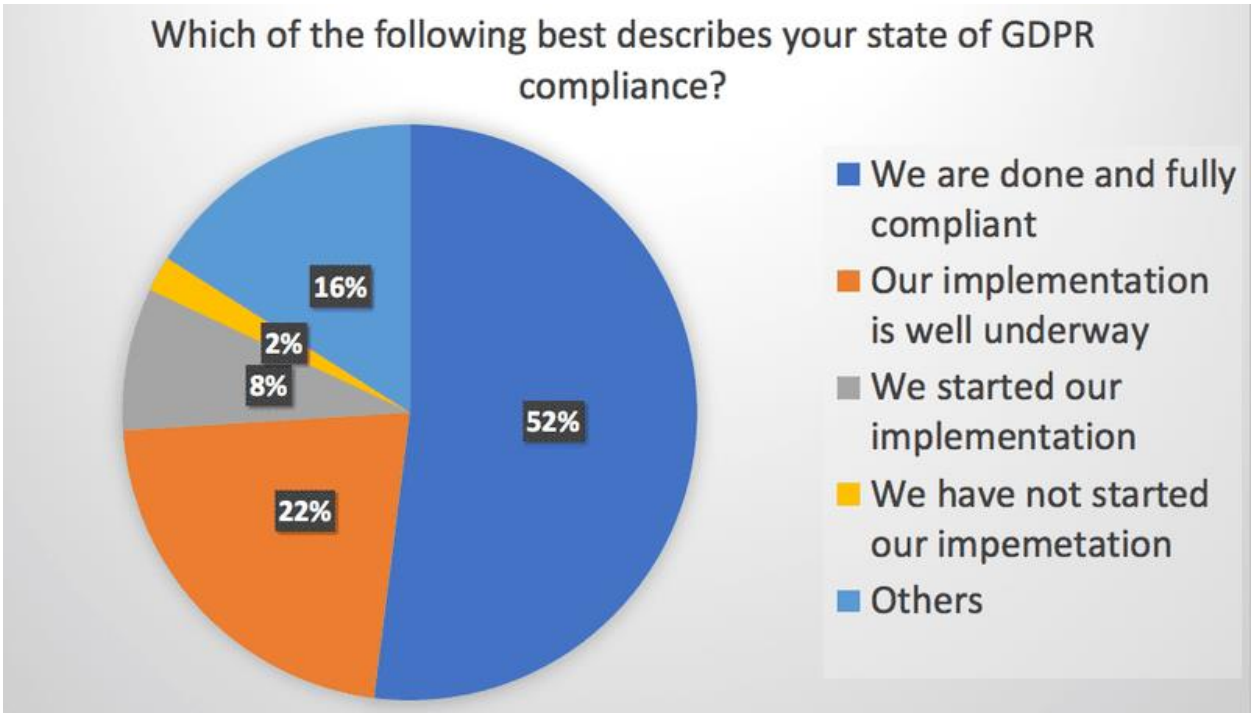

Figure 16. Current state of GDPR compliance [39]

Consequently, the GDPR is a significant risk for SMEs because it can impose heavy fines for non-compliance. The maximum fine for a GDPR violation is 4% of the organization's global annual turnover or €20 million, whichever is higher. Data breaches also have other negative

consequences for SMEs including damage to reputation and the resulting loss of customers, legal challenges and regulatory investigations.

SENTINEL enables SMEs to navigate the GDPR maze by:

1. **Helping them understand what personal data they collect and process** and the purposes for which they do so (via the assessment of their PAs)
2. **Helping them obtain consent for the processing of personal data,** which must be freely given, specific, informed, and unambiguous (via privacy policies)
3. **Helping them keep the collected personal data secure,** by taking measures to prevent unauthorised access, use, disclosure, alteration, or destruction of it (via the recommended OTMs)

4. Competitor Analysis

To date there is no holistic solution in the market capable of providing a unified framework, similar to SENTINEL, for (i) assessing SMEs/MEs current privacy and data protection risks, (ii) drafting and enforcing a unified GDPR-compliant privacy and data protection policy that addresses the identified gaps, (iii) collecting, analysing, and sharing critical privacy incident or data breach information over open-access platforms to enable both incident reporting and mitigation.

It is expected that the industry will progressively fill this gap, investing in specific solutions for the challenges that SENTINEL addresses. For the purpose of this analysis, we have identified some commercial solutions which share some SENTINEL features and could be considered competitors.

After analysing the existing options in the current market, we can establish three different competitor groups:

1. **Data protection compliance providers:** organisations focused on developing compliance solutions for GDPR, data protection and data privacy management.
2. **Cybersecurity providers:** organisations focused on delivering and/or monitoring digital security and managing data security compliance. A large number of companies offer such services in Europe and worldwide, so for the Competitor Analysis we have limited the analysis to companies which offer solutions similar to SENTINEL.
3. **Cyber range and other cybersecurity and data protection awareness and training providers:** organisations focused on simulating organisation security infrastructures and attack scenarios, conducting vulnerability assessments or providing gamified or other approachable content for cybersecurity and data protection awareness-raising and/or training.

4.1 Industrial competitors

4.1.1 GDPR and PDP compliance companies

There are several key players operating in the data protection market to address the growing demand for GDPR and personal data protection compliance. These players are offering software solutions across various applications including compliance management, risk management, preventing data breaches etc. Some of the key companies operating in the Data protection Market

include: One Trust LLC, AvePoint Inc, TrustArc, Securiti.AI. GDPRWise, BigID Inc, IBM Corporation, Protiviti Inc, RSA Security, DataGrail Inc, SureCloud, Vigilant Software, McAfee LLC, Microsoft Corporation, Symantec, Trend Micro, Palo Alto Networks, Cisco, Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, NetApp, Dell EMC, Hitachi Vantara, Acronis, Rubrik, Ctera, Cymulate, Deepwatch, Kaspersky, Avira, Quick Heal, Qihoo 360 [6,7].

4.1.2 Cybersecurity providers

The global cybersecurity market is witnessing significant opportunities and some of well-established key players include: IBM, Cisco, Microsoft, Palo Alto Networks, Fortinet, Check Point, Trellix, Trend Micro, Micro Focus, AWS, Oracle, Accenture, CyberArk, Zscaler, Sophos, Broadcom, F5 Networks[8,9]. The market is characterized by intensified rivalry among major players and fuelled by strategic partnerships & new product launches. For instance, in November 2023, IBM introduced a new product which integrated AI capabilities for threat detection, response enabling quick threat identification and management. Furthermore, Cisco introduced Secure Access in June 2023 to deliver a more secure user experience in complex and distributed IT environments[8]. In January 2024, Palo Alto Networks acquired CloudGenix to enhance its SASE capabilities. This acquisition extends Palo Alto Networks' Secure Access Service Edge (SASE) services, allowing them to provide more comprehensive and unified security solutions for Cloud-based data and applications[6]. In addition, Fortinet launched the "Cybercrime Atlas" initiative[10] to combat cyber threats and stop cybercrime globally.

It is worth mentioning that the emergence of several SMEs in the market, such as Argus, Checkr, Cloudknox[11], and DarkTrace[12], has exerted immense strain on established players to continuously launch new products with added functionalities to maintain revenue share and profitability. Cybersecurity start-ups are adopting the freemium model to penetrate various business verticals to increase their market presence, offering stiff competition to major industry rivals.

4.1.3 Cyber Range and simulation-based training providers

Regarding the Cyber Range market, the key players competing in the global market include: 360 Digital Security Group, Accenture, AIT, Cyber Peace, Deloitte Global, Ernst & Young, FengTai Technology, Field Effect, H3C, Integrity Technology, Keysight, CYBER RANGES, CybExer NSFOCUS, QIANXIN and Venustech, Kaspersky, RHEA Group, Cyberbit [13,14].

The table below presents the key SENTINEL competitors, their offerings by highlighting their interactions and key differences with the SENTINEL platform.

[6] https://www.verifiedmarketresearch.com/product/data-protection-market/
[7] https://www.fortunebusinessinsights.com/data-privacy-software-market-105420
[8] https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gad_source=1&gclid=CjwKCAjwouexBhAuEiwAtW_Zx8Gnw3yUrvANNnTHikkW7t1Tt6xuCJmAkQ16o4VrEH3d0jFFe_PE_hoC8fkQAvD_BwE
[9] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
[10] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-helps-launch-cybercrime-atlas-initiative
[11] https://cyberdefenseawards.com/top-100-cybersecurity-startups-for-2020/
[12] https://cybersecurityventures.com/cybersecurity-companies-list-hot-150/
[13] https://dataintelo.com/report/global-cyber-range-market/
[14] https://www.giiresearch.com/report/qyr1260756-global-cyber-range-education-market-research.html

Table 3. SENTINEL Industrial Competitors

Competitor	Description / Potential Synergy with SENTINEL
GDPR/PDP compliance companies	
OneTrust offers powerful and easy-to-use compliance solutions that are purpose-built to solve these challenges at scale – allowing organizations to simplify their privacy program management.	SENTINEL provides a one-stop shop platform for SMEs/MEs to choose from a plethora of services, (including GDPR CSA (GDPR Compliance Self-Assessment), ROPA (Records of Processing Activities), DPIA (Data Protection Impact Assessment), CSRA (Cybersecurity risk assessment)) that are tailored to their needs, infrastructure, and capabilities. Furthermore, the Cyber Range training service focuses on the easier and usable training service provision for SMEs/MEs, providing an economically viable solution for data privacy and compliance. In addition, the Identity Management system settles compliance and security issues and reduces the complexity of existing personal Data Management systems by allowing the SMEs/MEs to seamlessly interface with the platform for managing and processing personal information and data. Finally, it provides a set of open-source components and training materials that help SMEs/MEs to properly address security and privacy while providing capabilities to continuously monitor current and upcoming regulations in the field of security and privacy.
GDPRWise offers GDPR Compliance Software for the SME. The company provides SAAS software for small and medium sized organisations and their service providers.	
Vigilant Software provides tools to identify, understand and minimise the data protection risks and help to perform risk assessments. Furthermore, it offers a database of legal requirements and controls comprehensive support across its product range	
Proteus-Cyber offers a GDPR software privacy platform, offering a scored readiness evaluation, graphical illustration of compliance gaps, as well as recommendations for immediate action and insights.	In SENTINEL, the IdMS is totally independent of the platform used by SMEs or individuals, removing the need for third parties and integrations, whereas the Proteus tool audit 3rd party data processors. In addition, SENTINEL recommendations are for a) measures (OTMs) to be implemented, b) tools (plugins) to be employed and c) educational and training material to be studied.
GDPRBench is an open-source benchmark designed specifically to assess GDPR compliance of database systems to make it easy to understand and comply with digital privacy regulations.	SENTINEL contributes to tailor made GDPR compliance that considers the SME/ME's needs, infrastructure and requirements. It offers the organisation representative a human-readable and actionable policy draft with specific recommendations to be implemented, employed or to be studied.
Cyber range and simulation-based training providers	

CYBER RANGES delivers Cybersecurity Training and Capability Development Exercises for the management of Simulation-Based, Deep-Dive Experiences in Cybersecurity.	Contrary to current solutions that focus on large organisations or public authorities, SENTINEL's cyber range infrastructure is a hands-on training platform for simulations and education tailored to SMEs preferences based on their needs and infrastructure. The CyberRange gaming interface gives SME's the ability to test, evaluate, and train in real-world cyber threat scenarios as well as best practice, for data protection and GDPR. The user is automatically authenticated with OpenID and can create this session by themselves without any assistance and play the games at any time. In addition, these companies offer primarily cyber resilience and risk mitigation through continuous training and assessment. Whereas SENTINEL provides completed assessment processes appropriate to the SME profile parameters and proportional to the level of risk This part is not available in any of the currently existing solutions.
CYMPIRE™ CyWARIA is a Cloud-based serverless service for hands-on training. It offers ready-made training scenarios, also providing the capability to customize scenarios.	
Kaspersky Security Awareness is a custom-build software that simulates the impact that cyber-attacks and associated management decisions can have on business performance and revenue.	
Cybersecurity solution providers	
ForcePointDLP focuses on a unified data protection suite with a series of other features, such as automated policy enforcement, classification vendor compatibility and behavioural awareness.	The SENTINEL platform offers an end-to-end digital privacy / data protection compliance and impact assessment framework backed by cyber range-based testbeds to simulate data breaches, whereas ForcePointDLP is missing this part from its platform. SENTINEL's cybersecurity components (e.g., Security Infusion, MITIGATE) comprise a part of a holistic framework, covering the complete lifecycle of a company's data protection needs; from evaluation through scoring of their needs/infrastructure/etc to policy recommendations to a complete set of services and tools that are tailored to the enterprise. Furthermore, it provides training and education services for raising awareness for data protection and GDPR.
SPLUNK offers a platform that delivers among others application and infrastructure monitoring and compliance management.	
MicroFocus offers – among other- data privacy and protection with special focus on the identification, analysis and management of enterprise data and the establishment of policies towards data protection.	
EGNYTE offers content governance, privacy, compliance, and workflow automation with a single, turnkey platform.	SENTINEL has a collection of self-serving, state-of-the-art security- and privacy-enhancing modules, either open-source or contributed by SENTINEL partners, to address each policy point raised by the assessments and analyses, up to date with the latest intelligence via open-source repositories

	whereas EGNYTE offers pre-configured classification options for SEC, SOX, GLBA, HIPAA and other industry regulations.

4.1.4 European cybersecurity landscape

The ECSO Cybersecurity Market Radar [13] serves as a comprehensive visualization tool, marking a significant step forward in ensuring the transparency of the European cybersecurity market and boosting the visibility of its deployment-ready cybersecurity solutions and capabilities. With more than 200 European cybersecurity companies, **the ECSO Cybersecurity Market Radar presents a rich European cybersecurity industry landscape.**

The Radar is based on a market-oriented taxonomy of cybersecurity capabilities, developed by the ECSO working groups, dealing with market analysis, investments, cybersecurity companies and regions.

Based on their scope and designated capabilities, cybersecurity products and services provided by European-based companies present concrete competences and means to mitigate, resolve, monitor and analyse cyber-related threats and are categorized in the following capability levels:

- Identify (Figure 17): for the better organisational understanding of the IT infrastructure and cybersecurity readiness to manage cyber risks to individuals, systems, assets, data and capabilities.
- Protect (Figure 18): for appropriate safeguards to reduce the attack surface and to ensure the availability, integrity, confidentiality, auditability, and performance of the critical IT services. Wide range of 'protect' capabilities are provided by large European cybersecurity companies [discover it here], as well as by small and medium enterprises (SMEs).
- Detect (Figure 19): for appropriate tools to identify the nature and the scope of cyber-attacks carried out on the entity.
- Respond (Figure 20): for appropriate measures to effectively mitigate the detected cybersecurity incidents.
- Recover (Figure 21): appropriate action plans to bounce back from cyber-attack and to restore any capabilities or services affected.

For each level, there is additional categorization regarding the solution category and the product/service group each offering competes.

Figure 17. Identify: Product/Services segmentation [15]

[15] ECSO Radar: Identify

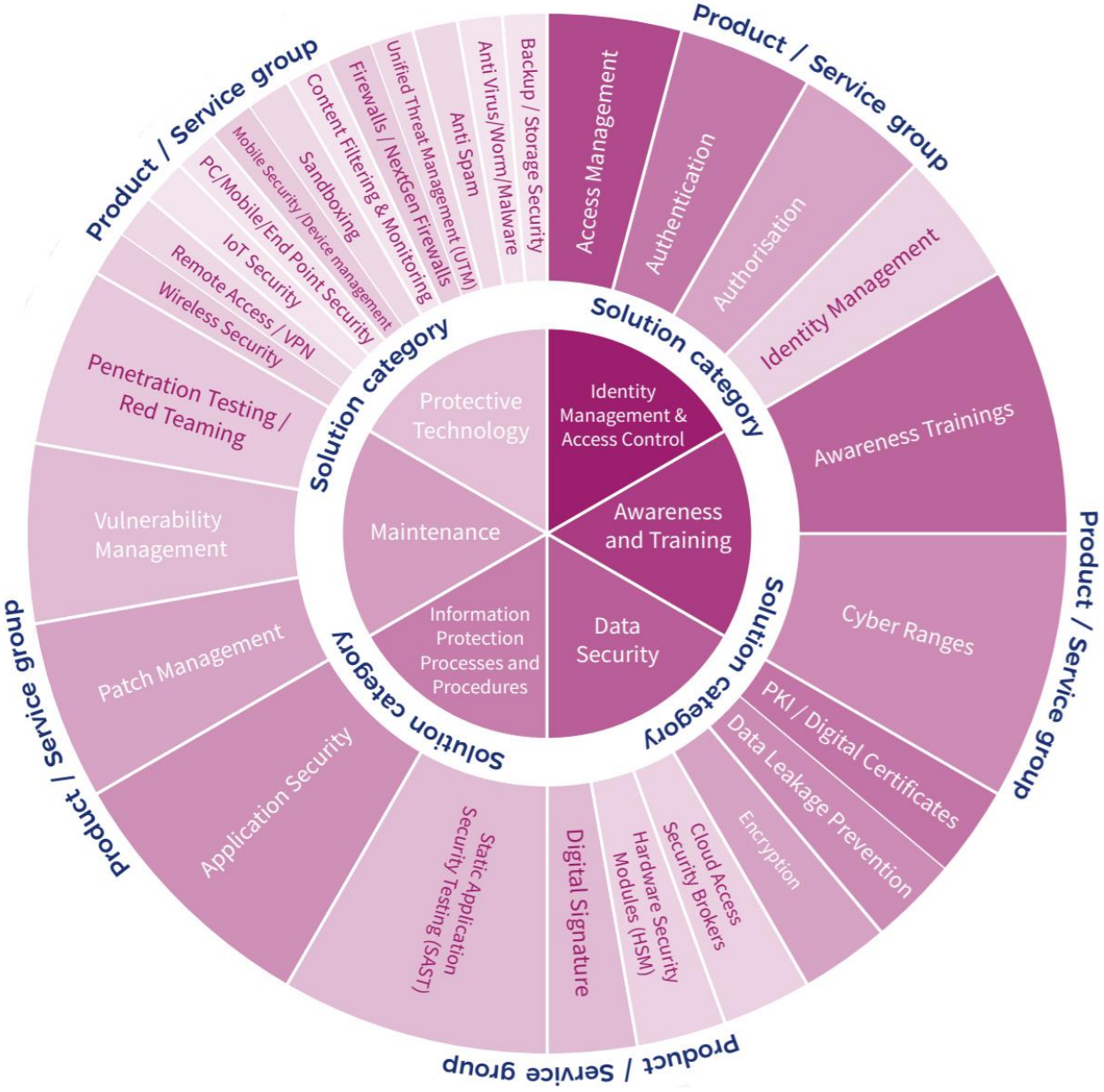

Figure 18. Protect: Product/Services offered by SMEs segmentation [16]

[16] ECSO Radar: Protect | Large Companies & SMEs

Figure 19. Detect: Product/Services segmentation [17]

[17] ECSO Radar: Detect

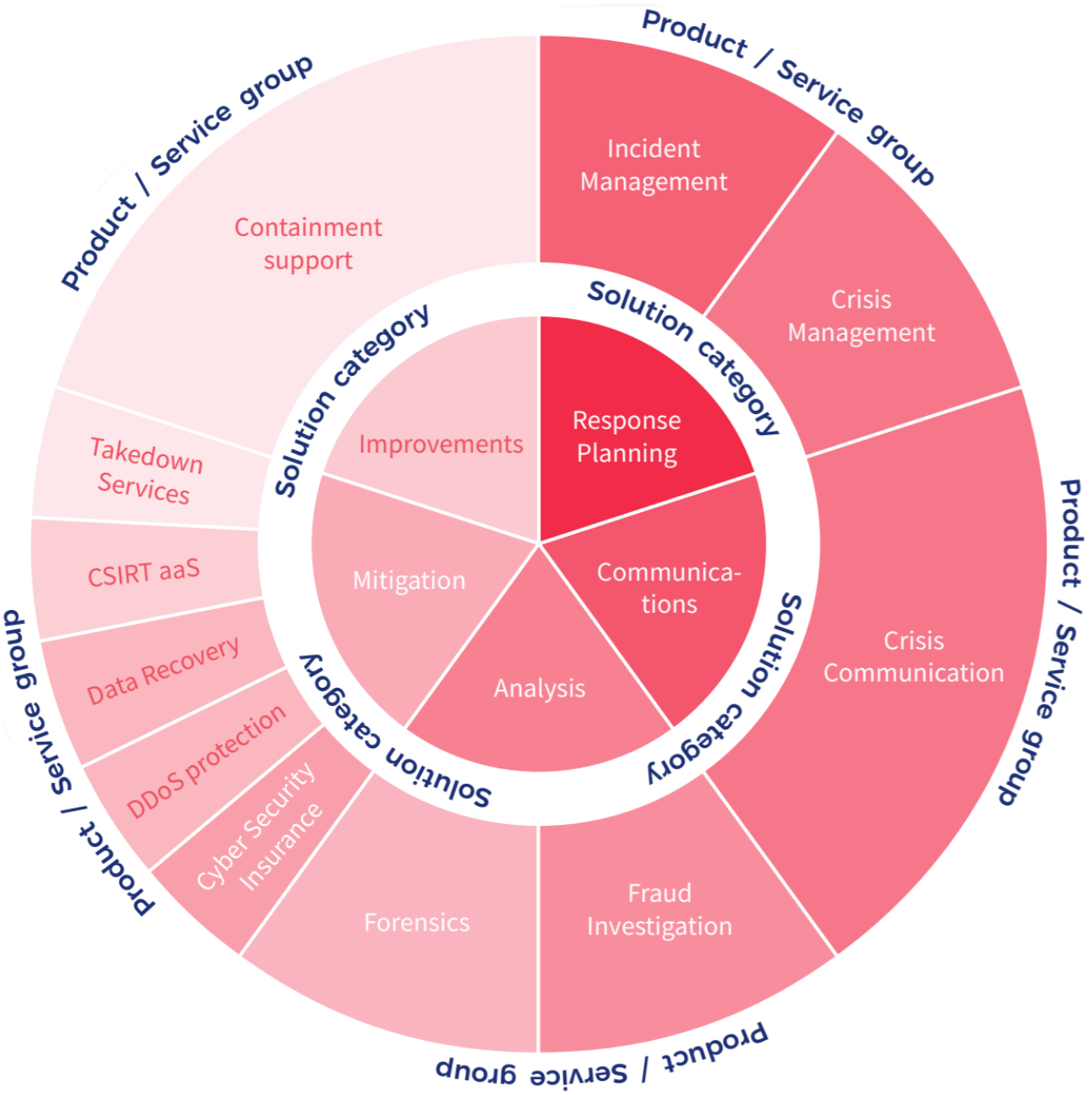

Figure 20. Respond: Product/Services segmentation [18]

[18] ECSO Radar: Respond

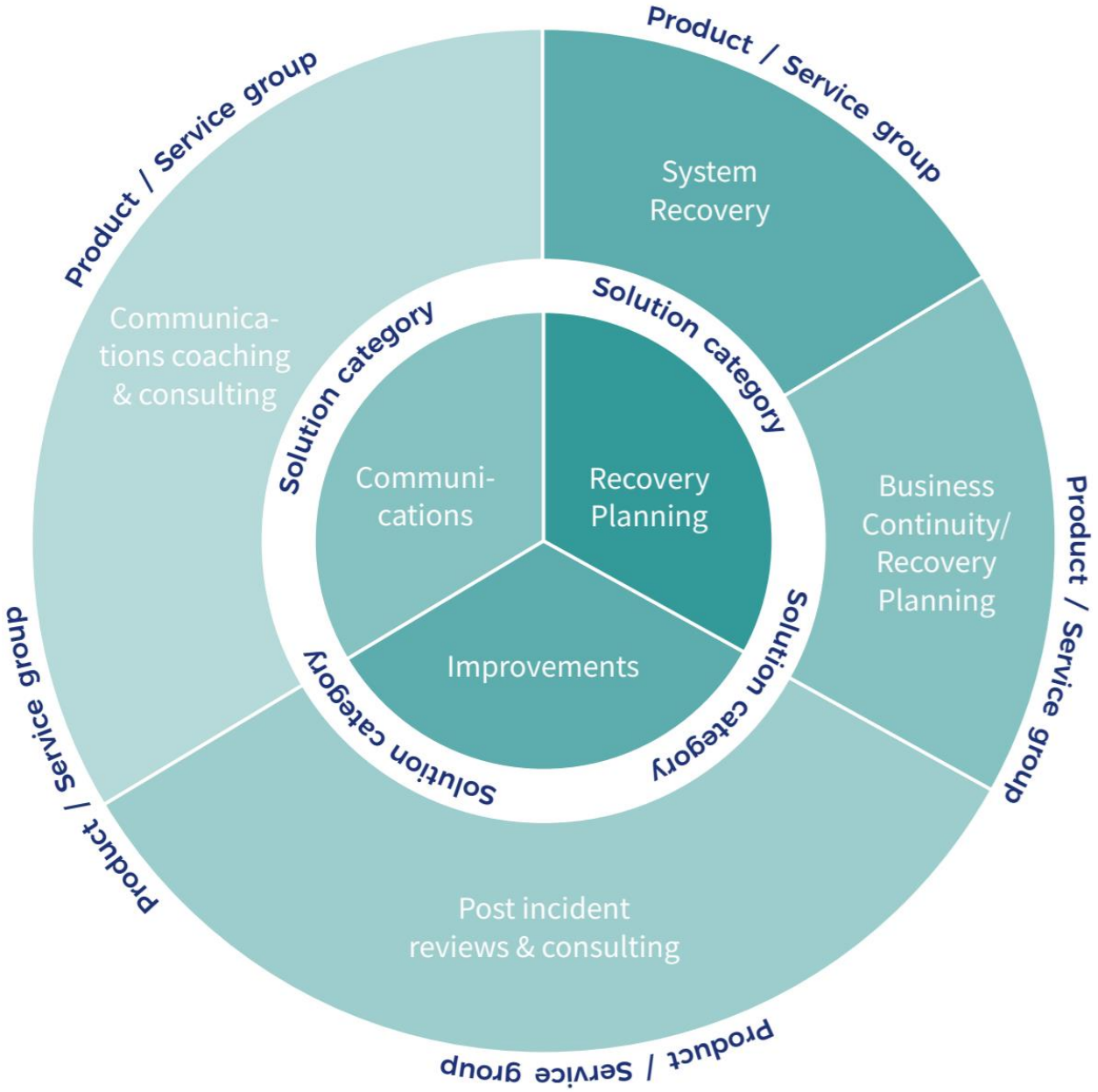

Figure 21. Recover: Product/Services segmentation [19]

In our market analysis, we are not aware of – at least we have not found – a software solution that offers an end-to-end digital privacy and data protection compliance self-assessment framework for SMEs into a unified digital architecture. The solutions currently found in the market cover only part of the functionalities offered by SENTINEL.

[19] ECSO Radar: Recover

SENTINEL is the only solution in the market that deploys a complementary set of data privacy, protection and compliance offerings, facing the challenges experienced nowadays by a vast majority of SMEs across Europe and potentially worldwide.

Figure 22. SENTINEL markets convergence

The competition in the sense described in the previous section offers their solutions as standalone or Cloud-based software which addresses specific aspects of CS and PDP, e.g., endpoint protection. By design, it's next to impossible for such offerings to address the bigger picture of tailored per-business requirements, training, CS awareness, smart recommendations, policy monitoring, a unified incident handling platform etc, aspects which are offered by SENTINEL.

4.2 Related projects

This section analyses the research and innovation projects positioned in the same topics as SENTINEL. Due to their relevance for the market analysis, these projects can act as competitors or collaborators depending on the context. The shared similarities as well as all synergies and collaborations made among these research projects and SENTINEL are summarised in the following table.

Table 4. SENTINEL-related projects

Project	Synergy with SENTINEL
PALANTIR[20] – Practical autonomous cyberhealth for resilient SMEs & Microenterprises (H2020 EU-funded, GA No 88335)	Both SENTINEL and PALANTIR target SMEs and MEs, nevertheless, PALANTIR focuses on privacy assurance, data protection, incident detection and recovery framework of highly dynamic service-oriented systems. To explore possible collaborations and further synergies PALANTIR was invited to participate in 1st Joint Clustering Webinar organised by SENTINEL in May 2022[21].

[20] https://www.palantir-project.eu/
[21] https://sentinel-project.eu/news-events/Clustering-Webinar-Security-Privacy-Data-Protection/

TRAPEZE[22] – Transparency, privacy and security for European citizens (H2020 EU-funded, GA No 883464)	SENTINEL and TRAPEZE have different objectives, primarily in terms of applied target groups; TRAPEZE focuses on the general public, while SENTINEL is tailored to SMEs/MEs. However, their common ground is the provision of a user-centric security and privacy resilience framework. SENTINEL together with TRAPEZE participated in 1st Joint Clustering Webinar in May 2022[21], Joint CyberSecurity Webinar in January 2023[23] as well as exchanged lessons learned and best practises in a roundtable discussion during the CitySCAPE project's final event[24].
PUZZLE[25] – Towards a sophisticated SIEM marketplace for blockchain-based threat intelligence and security-as-a-Service (H2020 EU-funded, GA No 883540)	Both SENTINEL and PUZZLE target SMEs/MEs and perform monitoring, forecasting, assessing and managing security, privacy and personal data protection risks, although each achieves this using different techniques. Both projects pursued synergies and further collaboration through various events including 1st Joint Clustering Webinar organised by SENTINEL in May 2022[21], Joint CyberSecurity Webinar in January 2023[23] and PUZZLE's Cybersecurity Conference in June 2023[26].
GEIGER[27] – Geiger cybersecurity counter (H2020 EU-funded, GA No 883588)	SENTINEL and GEIGER share a common interest to protect small business from cyber threats and offer tailor-made support for defending against them.
CYBERKIT4SME[28] – Democratizing a cybersecurity toolkit for SME (H2020 EU-funded, GA No 883188)	SENTINEL and CYBERKIT4SME share a common objective of helping SMEs/MEs analyse, forecast and manage cyber security, with the ultimate goal of making them more cyber-resilient. SENTINEL was engaged with CYBERKIT4SME and invited to take part in 1st Joint Clustering Webinar in May 2022[21].
SOTERIA[29] – User-friendly digital secured personal data and privacy platform (H2020 EU-funded, GA No 101018342)	The common ground between SENTINEL and SOTERIA is that they both follow a user-centric approach to create tools and services for secure personal data management, thought they are applied in different application domains and target groups.
TRUST AWARE[30] – Enhancing digital security, privacy and trust in software (H2020 EU-funded, GA No 101021377)	Both SENTINEL and TRUST AWARE aim to deliver a digital security and privacy framework to identify, audit, analyse, prevent and mitigate the impact of the various threats, however, the two projects leverage different technologies and apply to different domains. TRUST AWARE was among the 10 projects that participated in the "EU-made

[22] https://trapeze-project.eu/
[23] https://sentinel-project.eu/news-events/Joint-Cyber-Security-Webinar/
[24] https://sentinel-project.eu/news-events/SENTINEL-in-the-Final-Event-of-the-CitySCAPE-project/
[25] https://puzzle-h2020.com/
[26] https://sentinel-project.eu/news-events/SENTINEL-in-the-PUZZLE-International-Cybersecurity-Conference/
[27] https://project.cyber-geiger.eu/
[28] https://cyberkit4sme.eu/
[29] https://www.soteria-h2020.eu/
[30] https://trustaware.eu/

	cybersecurity for safe, resilient, and trustworthy applications and services" workshop in February 2023[31] as well as "Cyber Security and Data Protection Synergies" joint cluster event organised by SENTINEL in October 2023[32].
ARCADIAN-IoT[33] - Autonomous Trust, Security and Privacy Management Framework for IoT (H2020 EU-funded, GA No 101020259)	Both SENTINEL and ARCADIAN-IoT projects offer a solid framework for trust, security and privacy management however the two projects focus on different domains and target groups. The projects innovation capacities have been demonstrated during the ARCADIAN-IoT and SENTINEL final event in April 2024[34],[35].
Collabs[36] – A comprehensive cyber-intelligence framework for resilient collaborative manufacturing systems (H2020 EU-funded, GA No 871518)	SENTINEL took advantage and further exploited know-how, tools and technologies deployed within Collabs towards secure software environments.
THREAT-ARREST[37] – Cybersecurity threats and threat actors training – Assurance driven multi-layer, end-to-end simulation and training (H2020 EU-funded, GA No 786890)	SENTINEL exploited the advanced cybersecurity training methodologies and cyber ranges that were built in THREAT-ARREST and enhanced the similar services provided via the SENTINEL platform.
MISP[38] – Open-source threat intelligence platform & open standards for threat information sharing	SENTINEL used the data in MISP malware and information sharing platform to help SMEs be aware of the newest security Threats.
FORESIGHT[39] – Advanced cybersecurity simulation platform for preparedness training in aviation, power grid and naval environments (H2020 EU funded, GA No 833673)	SENTINEL exploited the scoring system and enhanced simulation capabilities and improved the SENTINEL platform.
CONCORDIA[40] – Cybersecurity competence for research and innovation (H2020 EU-funded, GA No 830927)	SENTINEL examined the work and results of CONCORDIA towards enhancing research and development in the area of information sharing for SMEs. We studied the possibility to integrate our platform with the one of CONCORDIA and currently the external sources available to the SENTINEL Knowledge Base (KB) are MISP and CONCORDIA MISP.

[31] https://sentinel-project.eu/news-events/SENTINEL-in-Joint-Workshop%e2%80%93EU-made-cybersecurity-for-safe-resilient-and-trustworthy-applications-and-services/
[32] https://sentinel-project.eu/news-events/Cyber-Security-and-Data-Protection-Synergies-Joint-Cluster-EU-Projects-Event/
[33] https://www.arcadian-iot.eu/
[34] https://sentinel-project.eu/news-events/ARCADIAN-IoT-and-SENTINEL-Symposium-and-Showcase/
[35] https://www.arcadian-iot.eu/arcadian-iot-and-sentinel-symposium-highlights-iot-cybersecurity-and-data-privacy-innovations/
[36] https://www.collabs-project.eu
[37] https://www.collabs-project.eu
[38] https://www.misp-project.org/
[39] https://foresight-h2020.eu/
[40] https://www.concordia-h2020.eu/

5. Identifying the SENTINEL Competitive Advantage

5.1 Intellectual property and assets per partner

To develop a joint business plan, it is important to map the intellectual property rights of each partner. This process identifies the technologies/plug-ins/KERs that each company brings to the project and helps better identify and articulate its competitive advantage and value proposition. The following tables list the updated inputs by partner as part of this process.

Table 5. Partners' updated IPR Scheme

Partner	Current IPR scheme
ITML	ITML has brought Security Infusion, Incident Handling and Sharing module (through Data Fusion Bus), as well as developed Recommendation Engine, Observatory, IdMS within the SENTINEL project. ITML's current IPR scheme supports that any knowledge and assets developed by ITML or brought to the project belong to ITML for exploitation and commercialization purposes.
LIST	GDPR-CSA designed and developed by LIST. Specific licensing agreement needs to be negotiated in fair and reasonable conditions.
IDIR	Knowledge produced explicitly by IDIR within SENTINEL is IDIR's intellectual property with regards to future commercialization. Technology and code will be open source.
INTRA	INTRA acts as an integrator in SENTINEL and does not bring any assets to the project.
STS	DPIA developed by STS provides the capability of automated self-impact assessments that identify the data protection risks of processing activities. The tool is subject to licensing.
AEGIS	FVT is the asset that AEGIS has already produced. FVT belongs to AEGIS for exploitation and commercialization purposes, according to AEGIS' present IPR structure. Furthermore, any information created specifically by AEGIS inside SENTINEL is both AEGIS intellectual property and AEGIS intellectual property in terms of potential commercialization.
TUC	TUC has contributed to the recommendation service through provision of open-source tools and courses. It is openly provided for SMEs/MEs, integrated version can be offered as SENTINEL commercial offerings.
ACS	ACS's current IPR scheme supports that any knowledge and assets already developed by ACS and brought to the project belong to ACS for exploitation and commercialization purposes.
UNINOVA	UNINOVA acts as a dissemination and communication manager in the SENTINEL project and does not bring any assets to the project.
CG	CG acts as a pilot owner in the SENTINEL project and does not bring any assets to the project. CG's main role is to test and validate the SENTINEL platform.
TIG	TIG acts as a pilot owner in the SENTINEL project and does not bring any assets to the project. TIG's main role is to test and validate the SENTINEL platform.
CECL	CECL acts as an ethics and legal advisor partner thus its main role is to examine and inspect the ethical and legal aspects within the project.

FP	FP brought the MITIGATE plug-in which is a simulation-based software for the identification, analysis and mitigation of cyber threats. The tool is subject to licensing.

Table 6. Partners' IPR Plans Beyond SENTINEL

Partner	IPR plans beyond the end of SENTINEL
ITML	Through SENTINEL, ITML wishes to further advance the tools and services that brings to the project, i.e., DFB used to design the Incident Handling and Sharing Module, Security Infusion, Identity Management System (IdMS), Intelligent Recommendation Engine and the SENTINEL Observatory. With regard to any advancements made on the individual assets that the company brings to the project as part of the SENTINEL's holistic framework, ITML plans to keep IPR of those assets and continue to exploit them. For the joint exploitation of the produced framework within the scope of SENTINEL, ITML will contribute to establishing standards for determining the rights and obligations of the SENTINEL partners, the creators of intellectual property and their sponsors, with respect to inventions, discoveries and work created. Towards this end, ITML together with Exploitation Manager of the project (STS) work on a preliminary exploitation agreement with involved partners regarding the management of knowledge and innovation derived as a result of SENTINEL.
LIST	GDPR CSA is an asset that contributes to the achievement of LIST's ambition regarding digital regulatory compliance which has proved to be an attractive tool gaining the interest of the business community. In this regard, LIST aims to seek new related research and innovation activities to extend and improve GDPR CSA technical and functional capabilities. In this regard, specific agreement needs to be negotiated to fairly and reasonably manage this asset beyond SENTINEL.
IDIR	The SCORE (Security Capabilities Oriented Requirements Engineering) methodology is IDIR's intellectual property with regards to future commercialization. The development of key contributed technologies to be used within SENTINEL's self-assessment framework for SME profiling and RASE scoring will be open source.
INTRA	As integrator of SENTINEL, INTRA aspires to exploit the delivered integrated framework, platform and acquired know-how together with the involved SENTINEL partners to obtain a competitive advantage in the field of security-sensitive services related to Cloud-based implementations and platform implementations, heterogeneous component integration and interoperability.
STS	STS has expanded the capabilities of the Security and Privacy Assurance Platform (SPAP) by designing and implementing the Data Protection Impact Assessment (DPIA) toolkit. STS will preserve the IPR of any developments provided to the SENTINEL project.
AEGIS	AEGIS intends to preserve the IPR of any breakthroughs achieved on the FVT that the firm provided to the project as part of the SENTINEL's holistic structure and continue to use it. AEGIS will contribute to the establishment of standards for determining the rights and obligations of the SENTINEL partners, intellectual property creators, and their sponsors with respect to inventions, discoveries, and work created, in order to facilitate joint exploitation of the produced framework within the scope of SENTINEL. AEGIS will reach preliminary agreements with

	relevant parties on knowledge management and IPR management in order to achieve this goal.
TUC	Through SENTINEL, TUC developed the recommendation service by providing open-source tools and courses. The service is openly provided for SMEs/MEs, integrated version can be offered as SENTINEL commercial offerings.
ACS	All development and content created specifically by ACS inside SENTINEL is both ACS intellectual property and ACS intellectual property in terms of potential commercialization.
CG	CG acts as a pilot owner in the SENTINEL project and CG's main role is to test and validate the SENTINEL platform. The acquired know-how and knowledge achieved with SENTINEL will be used to strengthen the competitive advantage of the company in the field of genomics.
TIG	TIG acts as a pilot owner in the SENTINEL project and its main role is to test and validate the SENTINEL platform. TIG will seek to fully integrate the SENTINEL final solution into each of the SMEs within the group.
CECL	CECL acts as an ethics and legal advisor partner thus its main role is to examine and inspect the ethical and legal aspects within the project. Beyond SENTINEL, CECL will exploit the results at academic level by providing relevant training seminars to students. Furthermore, CECL will widen the group of professionals that attend the GDPR issues through its training department and the provision of focused training seminars.
FP	In SENTINEL we provide our risk assessment tool where IPRs will be shared in all additional enhancements/developments around this tool with all partners involved in these developments

The table below lists and includes a short description of key exploitable results of each partner. These results are presented in D7.8 in more detail.

Table 7. SENTINEL Partners' Result(s)

Partner	Asset(s)
ITML	ITML exploitable tools and services within SENTINEL are: • **Security Infusion:** SI is an end-to-end, agent-based SIEM component, that performs real-time monitoring and alerting of hosts, services and security status in an IT infrastructure, as well as real-time security assessment based on process profiling, network scans and rule-based intrusion detection. The tool leverages state-of-the-art advanced visualization features to identify and assess vulnerabilities and suggest recommendation actions to limit potential risks. • **IdMS:** the SENTINEL IdMS solution is delivered via an implementation of authentication and Single Sign-On (SSO) based on the open-source solution Keycloak. The next step is to expand and generalize the solution to the personal data that SMEs/MEs manage for the end-users of their services that will be based on human-centric approaches (e.g. models like the MyData model) of managing personal data. • **Data Fusion Bus (DFB):** As part of the SENTINEL digital core, the incident handling, reporting and sharing module was delivered based on the Data Fusion Bus (DFB) offered by ITML that facilitates incident

	handling, reporting and sharing processes reported by the SENTINEL end-users. DFB is able to collect large amounts of both detected security notifications and incidents reported by end-users. • **Recommendation Engine:** As part of the SENTINEL digital core, the SENTINEL Recommendation Engine (RE) collects data of SMEs/MEs' processes, operations and infrastructure and provides a list of recommended organisational and technical measures (OTMs), plugins and trainings, to assist the organization address potential shortcomings and vulnerabilities. • **Observatory**: It is an intelligence knowledge hub, designed to provide a centralised threat intelligence knowledge base for cybersecurity, privacy and personal data protection, exchanging data in real-time among open security data platforms as well as aggregating anonymised information collected or produced within SENTINEL.
LIST	The GDPR Compliance Self-Assessment (CSA) module, developed by LIST, performs an automated analysis of both Processing Activities (PAs) and data protection organisational capability to determine whether personal data are handled in accordance with GDPR requirements. It automates standardized process assessment approaches based on a publicly available GDPR Assessment Model making assessment cheaper compared to expensive expert-based evaluation (audit, certification, etc) methods.
IDIR	IDIR's exploitable asset is the SCORE methodology. It is a unified solution that goes beyond the current state of the art and at the same time is aligned to the technical solutions offered by the SENTINEL technologies. The SCORE approach, specifically designed for RE (Requirements Engineering), and supported by appropriate modelling tools is based on a conceptual framework that uses as its key driving force the concept of 'capability'. In this approach, RE is seen as the transformation of current capabilities, which may be prone to security threats, to desired capabilities that mitigate these threats. Desired capabilities may be established either through internal developments or through acquisition of external capabilities from third parties. One of the advantages of SCORE is its focus on assets. Identification of enterprise assets facilitates the analysis of potential threats on these assets and associated risks that give rise to vulnerabilities that need to be evaluated and if necessary, to act upon as expressed by security goals. These security goals are realised in terms of capabilities that focus on security measures. The risk analysis process is based on mostly quantitative KPIs related to security goals.
INTRA	N/A. INTRA acts as the integrator in SENTINEL.
STS	In SENTINEL, STS through its Security Assurance Platform provides data protection and Impact assessment (DPIA). It is a self-assessment module that performs an automated assessment of Processing Activities. The tool leverages state-of-the-art advanced algorithms to calculate the likelihood, impact, and risk score, as well as, providing some quantitative metadata based on these metrics.
AEGIS	AEGIS's exploitable asset is the Forensics Visualisation Toolkit (FVT). FVT fosters cyber forensics and analysis of digital evidence. It helps operators to gain situational awareness and react fast in cases of security breaches as well as discover potential threats. It also acts as Network performance monitoring and diagnostic tool to provide a quick overview of an internal network's status and allow operators to monitor network performance and flowing traffic.

TUC	Within SENTINEL, TUC mainly contributed on the elements of recommendations for open-source tools and training materials. These include a list of open-source tools and available training material that can fill the identified gaps. For these elements, a wide list of open-source solutions and free courses have been identified in advance. Then, a model has been defined to specify the relevant technical or operational features that are provided by each of these offerings. The user can review this information through the main dashboards of SENTINEL.
ACS	ACS provides to SENTINEL the CyberRange, the CyberRange is a simulation and training platform. It is used in order to provide a cyber simulation environment in the objective of cybersecurity simulation and training purposes. It is based on a virtualisation environment managed through a graphical user interface aiming to build a representative system based on the SMEs/MEs IT system topology in order to test, evaluate and train in real-world cyber threat scenarios.
UNINOVA	UNINOVA acts as a dissemination and communication manager in the SENTINEL project thus it supports the project with it's knowledge and expertise related to dissemination, communication and stakeholder engagement activities.
CG	CG acts as a pilot owner. Its main role is to test the efficiency of SENTINEL and improve privacy and secure access of genomic data without negatively affecting ClinGenics productivity.
TIG	TIG acts as a pilot partner and aims to adopt the resulting platform to achieve the aims described in TIG exploitation goals.
CECL	CECL acts as an ethics and legal advisor partner with a main role to examine and inspect the ethical and legal aspects within the project, particularly focusing on key exploitable results related to data privacy and GDPR compliance. For this purpose, CECL has used its assets that are summarised below: • Deep knowledge of the new data protection legal and regulatory framework. • Long experience in providing focused and targeted trainings on GDPR regulatory framework to several professionals including judges, legal experts, DPOs, entrepreneurs etc. • Development of relevant training material. • Development of Manual Code of Practice to facilitate compliance with the legal framework for the protection of personal data. • Numerous publications on the subject matter. • Large network with research institutions, NGOs, academia worldwide.
FP	Within SENTINEL, FP has brought and enhanced its MITIGATE plug-in. It is a methodology and simulation-based software which enables the identification, analysis and mitigation of company-wide cyber threats. Moreover, it integrates a collaborative and standards-based risk management system which considers threats arising from their interdependencies, including potential cascading effects. It enables companies and other entities to manage security in a holistic and cost-effective manner, while at the same time it produces and shares knowledge associated with the identification, assessment and quantification of company-wide cascading effects.

5.2 PEST Analysis

The PEST (Political, Economic, Social, Technological) analysis is a business tool to discover, evaluate, organize, and track macro-economic factors which may impact SENTINEL. It examines opportunities and threats due to the different PEST strategic forces, thus helping strategic business planning.

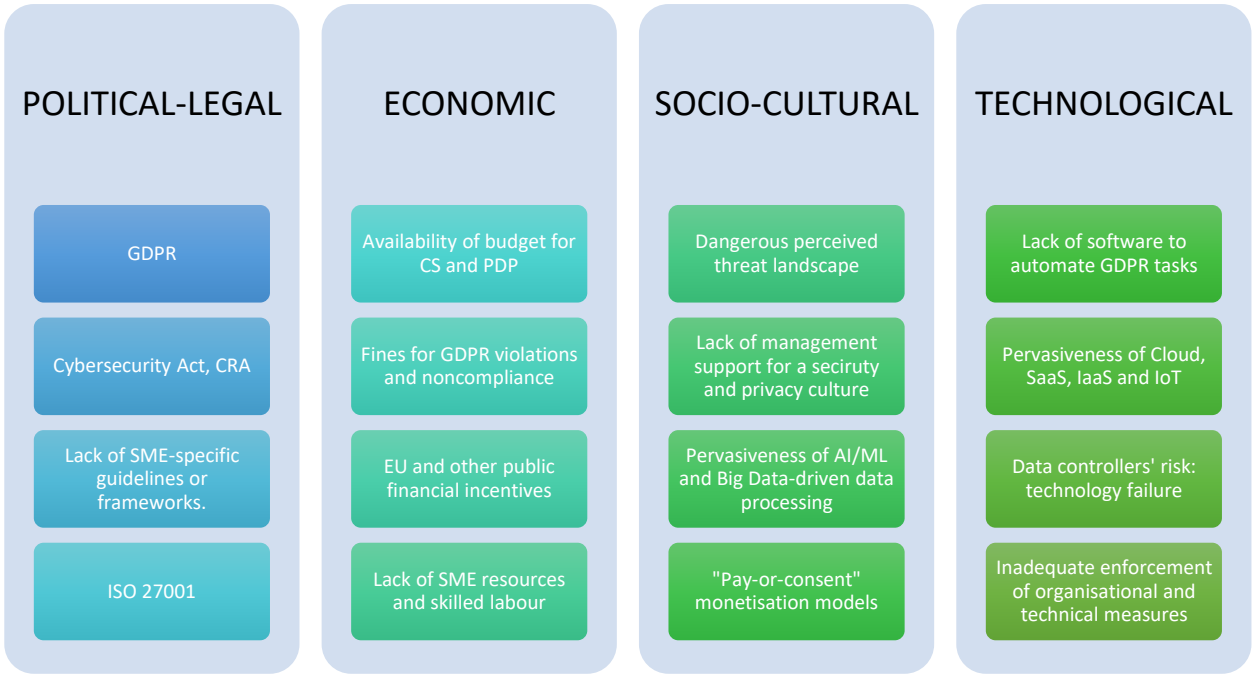

Figure 23. SENTINEL PEST Analysis

Failure to understand what drives demand in the cybersecurity and data protection markets can result in quick bankruptcy or the forced sale of a startup. As the SENTINEL project's R&I activities are about to be concluded, a robust understanding of what drives customer demand for related technologies, products, and services is a cornerstone.

SMEs in particular, as a rule, have fewer human, material, and financial resources. Resource allocation is prioritized to achieve the largest short-term gains, making it harder for them to respond to external factors in a strategic or long-term manner.

Supplier standards fall under the area of supplier requirements, and with the shift to just-in-time inventory and manufacturing, SMEs are being forced to adapt to satisfy these demands. External regulatory changes such as trade agreements, exchange rate fluctuations, and changes in government requirements force SMEs to adapt and adjust. Finally, profit erosion, export market potential, a desire to compete worldwide, and low barriers to entry in many of the industries where SMEs operate are all factors that compel them to adapt and change in order to survive.

The main external environmental triggers for change are government laws and regulations (as is the case with the GDPR and other compulsory data protection regulations), globalization of markets and the internationalization of business, major political and social events, technological

advancements, customer expectations, supplier requirements, increasing competition, organizational growth, and fluctuations in business cycles.

SENTINEL's PEST Analysis is presented in Figure 23 including the four factors that will be presented in the following subsections:

- **Political-Legal** factors (e.g. laws & regulations, both current and proposed, cybercrime, cyber terrorism)
- **Economic** factors (e.g. noncompliance fines, availability of skilled workforce, profitability, availability of startup capital or credit, and more)
- **Social and cultural** factors (privacy concerns, digital lifestyle, digital divide, "hacker" culture, etc)
- **Technological** factors (product lifecycles, the pervasiveness of Cloud computing, Internet of Things, etc.)

5.2.1 Summary of Political factors

Political factors include legislation, political stability, government policy, and activities of regulatory bodies and lobbying groups that may affect business through policies, rules, regulations and directives.

The predominant political-legal factor for SENTINEL is the GDPR, as well as upcoming cybersecurity-related legislation such as the EU Cybersecurity Act and the CRA. The complexity of the requirements and high outsourced cost, with uncertain outcomes, of compliance, provides a fertile ground for all the difficulties SMEs have, addressing these challenges. Additionally, a challenge for SMEs is the **availability and suitability of guidelines** for cybersecurity and data protection, in the form of standards, whitepapers or other and the **effectiveness of the policy instruments** to set the paradigm shift to cybersecurity and compliance. There are generic information and guidelines, such as "implement backup", or for example "appoint an information security officer and make sure that segregation of duties is applied" that address larger organizations with an existing cybersecurity framework where more specialization is possible. In addition, some of the well-known standards e.g., ISO 27001:201314 describe an approach for the design, implementation, operation, control and improvement of an Information Security Management System, which for many SMEs require external expert assistance to understand and implement.

Several EU bodies and Member States have issued guidelines in relation to cybersecurity, such as Information Security and Privacy Standards for SMEs [14] from ENISA, Europol's Safe Teleworking Tips and Advice [15] and CyberWatching [40]. EU's Tips for Cybersecurity when buying online [16], are not well known to SME owners, and a lot of the material is written to highlight the theory behind cybersecurity without providing practical guidelines. At the same time, the **digital transformation** of all types of businesses, including the SMEs, create new cybersecurity challenges and risks that should be addressed. COVID pandemic is forcing an even more rapid pivot to online ordering, remote education, home delivery, and remote and distributed work models, widening the attack surface of cybercriminals. Another political concern has to do with **responsibility and transparency issues**, a dimension that is highly connected with the lack of dominant framework and **standardization** schemes. For many businesses, customer experience is the key. In this context, they are willing to disguise cybersecurity and software

procedures in order to deliver a 'seamless customer experience'. Challenges arise when governments ask businesses, through compulsory legislation, to be more transparent and accountable, as is the case with the GDPR. Whilst companies may initially be reluctant to enter a maze of new regulations and incur additional costs only to document their data processing and police users' data and activity, most are still willing to comply in order to maintain a safe environment for employees, customers and partners, avoid fines and safeguard against reputational risk.

5.2.2 Summary of Economic factors

Economic factors include long-term trends of the global economy as well as fast market fluctuations, costs, competition, economic implications of political decisions, and taxation . As already highlighted in the previous chapters, a significant impactful factor is the **limited budget** that SMEs can invest in data protection and cybersecurity compliance. Preparedness efforts entail investments from various aspects such as awareness, training, implementation of privacy, data protection and cybersecurity organisational and technical measures and engaging external experts. **Dedicated GDPR compliance and cybersecurity solutions**, such as compliance assessments and monitoring, ROPA software, DPIA audits, data mapping and data processors / third party / vendor data management, data subject requests management, security technical measures such as privacy-enhancing technologies (e.g. encryption, anonymisation and data obfuscation), advanced firewalls or security information and event management systems (SIEM) can all be very large investments, especially for SMEs.

While many SMEs have engaged with the Cloud under SaaS or IaaS models, due to their size many SMEs often do not qualify for special offers and have to deal with fixed cybersecurity SLA contract clauses which are hard to understand and assess, unable to reach the SLA flexibility dedicated to large organizations. Advanced solutions offering a great variety of abilities and possible customizations useful for more secure and GDPR compliant organizations, are often not used by SMEs due to SMEs not being aware of understanding the solutions offered. In many cases, the security and privacy offering services are often part of high-level subscription plans which may not be suitable to an SME. While not specific to the cybersecurity challenges posed by the COVID-19 pandemic, it is evident that many SMEs view cybersecurity and GDPR compliance as a cost rather than as an investment in their business.

For many SMEs, a **lack of financial resources** and a **lack of skills** including managerial skills reduce the likelihood of adopting basic or advanced cybersecurity/data privacy/data protection/GDPR compliance-related measures. Moreover, uncertainty about future digital standards, internal resistance to change, regulatory obstacles or IT issues are barriers to understand and adopt security mentality and regulatory compliance attitude. For these reasons, it is expected the intensification of activities that bring together EU citizens, Member States, the European Commission, EU bodies, and governmental organisations, the private sector and academia to promote healthy cybersecurity habits. Online activities, including trainings, conferences, presentations and national campaigns, across Europe, and beyond, are held to boost awareness of cybersecurity risks and share the up-to-date guidelines and ways to mitigate them. The Commission has further strengthened its approach by including cybersecurity at the heart of its political priorities: trust and security are at the core of the Digital Single Market Strategy [17], while the fight against cybercrime is one of the three pillars of the European Agenda on Security [18].

The GDPR scene is taking shape across Europe, with regulators implementing the laws for various violations. The magnitude of the GDPR implementation is highlighted by the **growing fines imposed on various businesses**. The GDPR provides the DPAs with different options in case of non-compliance with the data protection rules:

- likely infringement – a **warning** may be issued;
- infringement: the possibilities include a reprimand, a temporary or definitive ban on processing and a fine of up to €20 million or 4% of the business's total annual worldwide turnover.

It is worth noting that in the case of an infringement, the DPA may impose a monetary fine instead of, or in addition to, the reprimand and/or ban on processing.

The authority must ensure that fines imposed in each individual case are **effective**, **proportionate** and **dissuasive**, and consider factors such as the nature, gravity and duration of the infringement, its intentional or negligent character, any action taken to mitigate the damage suffered by individuals, the degree of cooperation of the organisation, etc.

Fines related to GDPR infringement and non-compliance, all over the EU, have cumulatively exceeded the amount of EUR 4.5 Bn as of April 2024, having tripled since just 2 years before (April 2022 ~ EUR 1.6 Bn)[41].

Although by far the greatest share of these fines for violation or noncompliance have been imposed on large and prominent tech companies such as Meta, Amazon, TikTok and Google, SMEs are by no means exempt. In terms of sheer numbers, SMEs are the largest group to be fined for GDPR-related violations and the fines range roughly between EUR 1000 and EUR 2 Mn.

Sector	Sum of Fines
Media, Telecoms and Broadcasting	€ 3,313,401,366 (at 293 fines)
Industry and Commerce	€ 912,615,001 (at 450 fines)
Transportation and Energy	€ 87,589,710 (at 110 fines)
Finance, Insurance and Consulting	€ 61,868,558 (at 217 fines)
Employment	€ 59,471,177 (at 133 fines)
Public Sector and Education	€ 27,793,063 (at 238 fines)
Accomodation and Hospitalty	€ 22,490,048 (at 65 fines)
Health Care	€ 16,969,709 (at 197 fines)
Real Estate	€ 2,601,831 (at 60 fines)
Individuals and Private Associations	€ 1,860,566 (at 278 fines)
Not assigned	€ 1,767,208 (at 124 fines)

Figure 24. Cumulative GDPR fines by sector, by sum of fines (May 2024)[42]

[41] https://www.enforcementtracker.com/
[42] https://www.enforcementtracker.com/?insights#countrystatistics

Sector	Number of Fines
Industry and Commerce	**450** (with total € 912,615,001)
Media, Telecoms and Broadcasting	**293** (with total € 3,313,401,366)
Individuals and Private Associations	**278** (with total € 1,860,566)
Public Sector and Education	**238** (with total € 27,793,063)
Finance, Insurance and Consulting	**217** (with total € 61,868,558)
Health Care	**197** (with total € 16,969,709)
Employment	**133** (with total € 59,471,177)
Not assigned	**124** (with total € 1,767,208)
Transportation and Energy	**110** (with total € 87,589,710)
Accomodation and Hospitalty	**65** (with total € 22,490,048)
Real Estate	**60** (with total € 2,601,831)

Figure 25. Cumulative GDPR fines by sector, by number of fines (May 2024)[42]

Country	Number of Fines
SPAIN	**838** (with total € 79,998,030)
ITALY	**354** (with total € 149,444,327)
GERMANY	**183** (with total € 55,463,233)
ROMANIA	**176** (with total € 1,130,950)
POLAND	**73** (with total € 3,944,269)
GREECE	**68** (with total € 34,247,140)
HUNGARY	**68** (with total € 2,518,861)
NORWAY	**51** (with total € 12,117,950)
FRANCE	**45** (with total € 371,699,300)
CYPRUS	**42** (with total € 1,429,000)

Figure 26. Cumulative GDPR fines by country, by number of fines (May 2024)[42]

Country	Sum of Fines
IRELAND	€ 2,855,363,400 (at 27 fines)
LUXEMBOURG	€ 746,314,000 (at 32 fines)
FRANCE	€ 371,699,300 (at 45 fines)
ITALY	€ 149,444,327 (at 354 fines)
SPAIN	€ 79,998,030 (at 838 fines)
UNITED KINGDOM	€ 75,532,800 (at 14 fines)
GERMANY	€ 55,463,233 (at 183 fines)
GREECE	€ 34,247,140 (at 68 fines)
SWEDEN	€ 26,462,230 (at 38 fines)
THE NETHERLANDS	€ 24,924,500 (at 24 fines)

Figure 27. Cumulative GDPR fines by country, by sum of fines (May 2024)[42]

As illustrated in Figure 26, Spain, Italy, Germany and Romania have the largest number of fines, most of which have been levied on SMEs, while Ireland and Luxembourg are leading by sum of fines, indicating that the larger organisations reside there, with fewer fines adding up to much larger sums per fine imposed.

5.2.3 Summary of Social factors

Social factors refer to the social and cultural conditions of individuals or groups. These are reflected in attitudes, preferences and trends that can influence market behaviour and political decisions and eventually legislation. It is therefore important to understand how social factors may influence market demand, funding possibilities and legislation in order to determine how they may affect the future business environment. The relevant social factors and the society of interest will depend on case to case. It is also good to note that the social factors may change quickly, for example, as employment or economic conditions change.

Cybersecurity/data privacy/data protection are complex issues connected with technical solutions and measures; it is often perceived that they only concern IT related people. **Low cybersecurity/data privacy/data protection awareness of the personnel is a market impactful factor, and** each person should have at least basic awareness regarding these aspects and how their attitude can affect the relevant posture of the entire organization. What is really needed is a transition from initial awareness to internal culture. For example, SME personnel should know and understand how spear phishing and other social engineering attacks work, what constitutes personal/sensitive data, how they can create secure passwords for their data, and other basic cybersecurity precaution/data privacy/data protection measures.

While not specific to the IT-related challenges posed by the COVID-19 pandemic, it is evident that many SMEs view cybersecurity/data protection compliance as a cost rather than as an investment in their business. Compounding the challenges in this area is that many relevant solutions **require specialized IT knowledge** to implement and manage them properly. All of these issues combined

make managing cybersecurity/data protection compliance within a SME a big challenge. Relevant vendors should also be required to ensure their products are secure by default, provide adequate data protection/privacy and that managing these products should be relatively straightforward for non-technical people.

With the rising number of vulnerabilities and threats, contributing to an overly **ominous threat landscape**, the need for effective cybersecurity is growing exponentially. Outdated network security solutions are not enough in securing enterprises from advanced threats. Factors such as a lack of cybersecurity experts are key. The high cost of implementing and updating security solutions impedes the adoption among small and medium enterprises (SMEs).

A key success factor for any business initiative within a company, no matter its size, is **having senior management support** for that initiative. It is well known that without management support any initiative will flounder and eventually fail. This is particularly true with cybersecurity as it can be very hard to convince management to invest time, resources and money into something that is hard to demonstrate brings direct value to the business. While in larger organizations senior management can rely on their own cybersecurity experts or bring that expertise into the organization using consultants, many SMEs do not have this luxury. Instead, senior management within an SME often rely on their own knowledge of issues or what they learn from their peer networks. As such, there is low awareness amongst SMEs that they face many cybersecurity threats with many of them thinking they “are too small for criminals to want to hack them.” Contrary to a concept that cyber-attacks occur only to large organizations, all enterprises can be similarly attacked, regardless of their size and stored information. SMEs are an interesting target for cyber-attacks, because criminals may consider them to be easy targets due to SMEs not having robust cybersecurity measures in place. In addition, as many SMEs provide services to larger organizations an SME could be of interest to cybercriminals as a way to attack the supply chain of this larger organization.

Considering **data protection requirements**, SMEs handle a variety of personal information: customer information, details about production, procurement details, financial data, policies, procedures, and other, including sensitive information such as children or employee or medical data, data revealing political preferences, racial or ethnic origin, biometric data and potentially many more, with the added fact that sometimes these data undergo innovative machine-drive mass processing to enable automated or ultra-fast decision making. GDPR call for SMEs to understand and document their personal data processing in detail, always keep these records up to date, enable data subjects to exercise their fundamental rights which concern how their data is processed or exploited, keep them notified of potential data breaches and, of course, always be transparent and accountable as to how the data processing is protected by specific organisational and technical measures.

From a socio-cultural perspective, the data protection requirements may also be viewed in terms of a few other key factors such as:

- the pervasiveness of data-driven decision-making, leveraging machine learning and AI,
- the intricacies of defining a right to privacy vs a right to data protection, and whether the latter is a component of the former, and
- the potential dangers of the **commercialisation of data protection in the case in “pay-or-consent” business models**, whereby companies seek to make money offering end-

users the alternatives to either they pay for their offering (e.g. social media, content, etc), or allow the placement of personalised advertising, which competes for users' attention and oftentimes disregards critical data protection requirements and considerations.

5.2.4 Summary of Technological factors

Digitalization of all sectors of society and business has been the dominant trend for quite some time and will continue to accelerate and challenge conventional solutions by disrupting business models and offering increased capacities at lower costs.

Digital technology, by putting individuals' fundamental rights at risk, enables the principal problem that data protection regulations are trying to solve. As such, it is obvious that, **as well as being the problem, technology must also provide the solution**. If organisations are storing too much personal data, for example, technology needs to apply data minimisation and/or help data subjects exercise their rights to limit or stop the processing altogether.

In practice, however, despite technology being both the problem and the solution, actual IT systems used by organisations today have not been designed or deployed with data protection requirements in mind. This is why we see so much debate over the retention and storage of personal data, so much confusion about the nature and whereabouts of personal data and so many technology-related cyber-security failures. In essence, the technology stack (a way to formalise the technical measures) may be seen as the missing link in actually enforcing privacy and data protection. The underlying reasons vary but today, with GDPR enforcement fully underway and tougher potential for scrutiny, instances of technology failure will be harder to excuse.

GDPR Art. 24 (1): Responsibility of the controller: Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, ***the controller shall implement appropriate technical and organisational measures*** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

The predominant technological factor driving the enforcement of data protection requirements and enabling accountability for organisations are the Organizational and Technical Measures (OTMs), a concept brought forward from various security frameworks and cybersecurity standards to apply in data protection as well, are guidelines or recommendations which dictate how personal data may be processed (captured, grouped, consulted, altered, used, deleted, and so forth) of with the aim of meeting the appropriate (risk-based) cybersecurity and data protection requirements outlined by the GDPR. They cover many subject areas present in the digital and physical environments. OTMs address GDPR compliance-related aspects such as privacy policies, managing consent, DPIA, the assignment of DPOs and data protection responsible persons, managing data subjects' requests, managing third-party data processors and vendors, but also technical and cybersecurity aspects such as secure communications, encryption, data obfuscation, secure IAM and user accounting, strong passwords, backups and business continuity, firewalls, antivirus and anti-malware, biometrics, secure data erasure, physical access and many more. SENTINEL specifically addresses 10 organisational and 10

technical categories, and intelligently recommends over 170 OTMs based on risk and a number of custom rules, all detailed in the project's deliverable D3.3, Section. 5.3.

5.3 SWOT analysis

The SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats) aspires to identify the "internal" strengths and weaknesses of SENTINEL (Figure 28) and its "external" opportunities and threats. It is a strategic tool helping SENTINEL identify factors that may be favourable or unfavourable during a go-to-market and scaling. The SWOT analysis identifies:

- The **strengths** of the offering itself, especially in terms of its unique value proposition, completeness of features and usability;
- The **weaknesses**, which will have to be addressed and mitigated as plans for fundraising and commercialization materialise;
- Potential **opportunities** to be exploited during commercialisation; and
- Potential **threats** to market success, to be considered.

5.3.1 Strengths

The strengths of SENTINEL primarily lie in its core value propositions. The way GDPR and data protection compliance is addressed substantially differentiate it from that of competitors and allow SENTINEL to boast a high degree of assessment and monitoring automation, evidence-based documentation of accountability (especially with regard to the recommendation and implementation tracking of organisational and technical measures), ongoing and sustainable monitoring, and streamlining internal (processing activity records) and external (DPIA and other audit-related) data protection reporting. Although SENTINEL's features mostly overlap with GDPR compliance-related competitors, SENTINEL can boast of lower costs coupled with more automation, ease of use and a more comprehensive and intelligent process for recommending measures. These strengths are coupled with the combined and complementary expertise of consortium partners in the sectors of data protection, privacy, cybersecurity, software and usability engineering, Cloud integration and deployment, legal support and many more. Consortium partners have brought a large number of mature offerings and related intellectual property into the project, as is the case with ITML's Security Infusion and Airbus' CyberRange both of which are high-TRL and high-MRL products, with a successful track record in the market.

5.3.2 Weaknesses

SENTINEL's primary weakness lies in the complexity associated with implementing a joint commercialization of the project, based on a loosely described consortium agreement having to consider a relatively large number of IP restrictions and potentially conflicting aspirations of different partners having contributed to the project. Such conflicts cannot be easily resolved in the course of the R&D project itself, where no external investment or monetary gains are foreseen. A well-structured business plan, with clear IPR management, promoting the unique selling proposition of SENTINEL and the clear joint exploitation goals will help alleviate this weakness.

A secondary consideration is the lack of certain data protection features which competition possesses. These may be identified as: (a) Processor/third party and vendor management, (b) Data subject requests management, (c) privacy policy and consent management. The addition of these features will allow SENTINEL to face the competition from a better standpoint.

Looking into additional weaknesses, we can identify (i) the lack of internal resources and funding to bootstrap the go-to-market activities without significant successful external fundraising, (ii) the potential to further narrow down the target audience and (iii) to further clarify its value proposition.

5.3.3 Opportunities

The landscape external to SENTINEL does present a number of potential opportunities which we'll attempt to identify below:

A) **A rising need for data protection compliance-related offerings combined with a relatively underserved market**. Cybercrime, including malicious or ransomware-driven data breaches with extortion, is constantly on the rise, and smaller businesses are largely vulnerable as has been sufficiently demonstrated by the number and severity of incident and well as the steeply rising number and aggregated amount of fines related to GDPR violations and noncompliance. The market for GDPR and data protection software solutions in general can be considered as *emerging* and not an established or mature one, which provides a clear opportunity for SENTINEL.

B) **Unclear value proposition and audience targeting by competitors**. Although direct competitors -of all sizes- are not few in number, due to the very nature and complexity of data protection compliance, their value proposition and intended audience is often unclear, i.e. whether they are addressed to professional DPOs, lawyers or internal company stakeholders, executives or staff. SENTINEL can clearly benefit from this lack of clarity by articulating a robust, concise and simple USP addressed to the right audience.

C) **GDPR awareness activities are abundant**. Awareness initiatives at the global and European level are only increasing in number and impact, providing ample opportunity for SMEs to consider cybersecurity and GDPR compliance as an integral part of their operations, indirectly promoting SENTINEL's proposition. For example, the European Cybersecurity Month (ECSM) [41] is the European Union's annual campaign dedicated to promoting cybersecurity among citizens and organisations, and to providing up-to-date digital security information through awareness raising and the sharing of good practices. Similarly, GDPR and privacy awareness courses (e.g., [42]) help employees learn about rules, principles and best practices regarding privacy and personal data protection, thus reducing the risk of GDPR breaches. The raise-awareness activities include conferences, workshops, trainings, webinars, presentations, online quizzes and more, providing resources for citizens to learn more about protecting themselves online.

D) **An answer to overall complexity**. The digitalization of companies is often accompanied by the increased complexity of IT tools and ICT infrastructure. The new way of SME operations requires the compliance of regulations and GDPR requirements, making it harder for SMEs owners to understand the emerging cybersecurity risks and comply with the law. In many cases, their driving force is the fines they have to pay in case of regulation inconsistencies instead of the full understanding of the value of personal data protection. The aforementioned challenges are market opportunities for SENTINEL as it provides a one-stop-shop for SMEs for their early and more advanced steps to cybersecurity and regulatory compliance.

5.3.4 Threats

The landscape external to SENTINEL does present a number of potential threats which we attempt to identify below:

A) **Number and size of competition**. The effectiveness of SENTINEL's business proposition is analogous to that of its competitors. Even though, as mentioned above in opportunity (B), competitors' USP and targeting may still be unclear, they keep increasing in number from a few consolidated offerings back in 2020 to a much larger number today (2024), also resulting from a consolidation in the sector with large and established compliance software suites acquiring smaller GDPR-specific software developers and integrating their offerings. Taking into account that customers will have a tendency to trust established players and more mature offerings, it will be harder for SENTINEL to compete in this marketplace in lack of an established track record, without a very clear differentiating USP, as the market pace picks up.

B) **Changing regulatory environment**. The GDPR law in itself will be subject to frequent changes but the way the DPAs and other bodies interpret it will, as well as the arsenal of available technologies, OTMs, tools, software and trainings available. This, combined with an evolving cybersecurity threat landscape is an important factor. The offered policies, OTMs, trainings, tools, and other recommendations should be always up to date, at the risk of potentially failing to address emerging data protection requirements sufficiently, with all the added external cost but also business risk for SENTINEL this incurs.

C) **Potential negative coverage or customer testimonials**. The possibility of receiving negative feedback from either a publication, public event or in a customer review is always present. In the early stages of a startup such as SENTINEL, negative publicity is harder to mitigate and needs to be sufficiently addressed as an external risk.

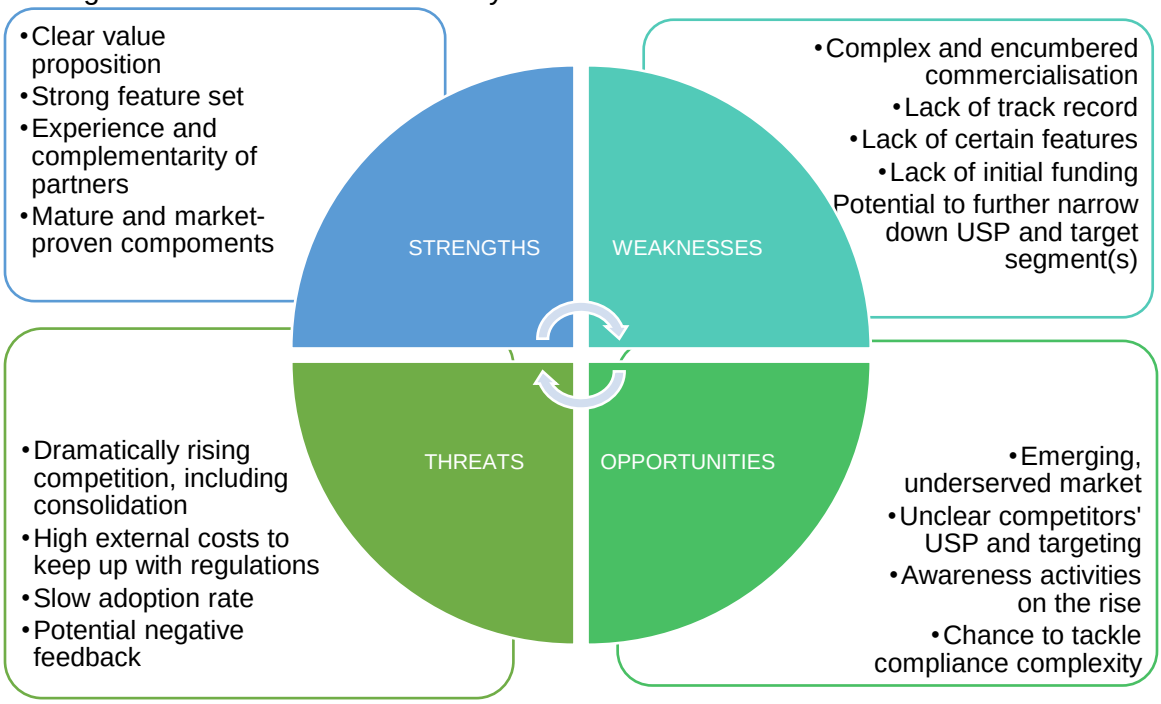

Figure 28. SENTINEL SWOT Analysis

5.4 Final value proposition

SENTINEL is a one-stop shop for GDPR and overall data protection compliance, backed by bundled as well as external or recommended tools and trainings. It is addressed to smaller organisations, offering them four distinct value propositions:

(a) To **educate** themselves about GDPR's data protection requirements and, specifically, why individuals' data and privacy need protection, how the personal data processing activities may affect data subjects' privacy, and what needs to be done in terms of organisational and technical measures (what GDPR refers to as the security of personal data), complemented with training and educational material for cybersecurity, data protection and privacy.

(b) To become **compliant** through accountability by documenting (keeping records of) evidence supporting their GDPR compliance claims. Specifically, SENTINEL offers: a Record of Processing Activities (ROPA) to help businesses comply with Art.30 of the GDPR for keeping records of how personal data is processed and the nature and intention of data processing activities; as well as and a mapping between the identified data protection requirements and the specific recommended organisational and technical measures, training material and software & tools to satisfy them.

(c) To **reduce costs through automation** by acquainting key business and technical people in the organisation with data protection compliance principles, thus saving on consultancy, training and education costs. As an example, an SME stakeholder, after having completed a SENTINEL user journey, will have a more holistic understanding of the EU's data protection requirements, their own organisation's GDPR compliance assessment, the estimated risk associated with their Processing Activities and organisation as a whole and what specific measures need to be put in place to strengthen their compliance and their whole privacy and security stance.

(d) To **strengthen their cybersecurity through awareness and training** via enterprise-grade and well-integrated tools, adapted for smaller businesses, such as the CyberRange and the CRSA (Mitigate).

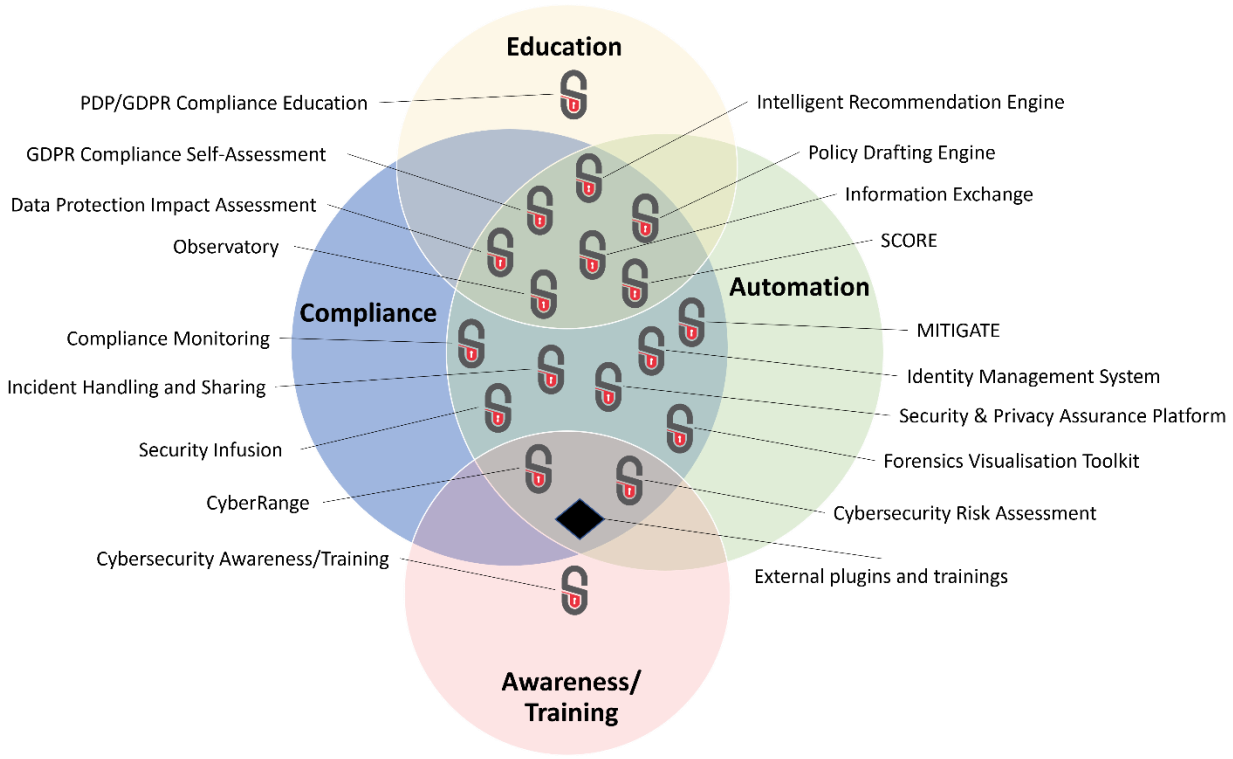

Figure 29. SENTINEL value propositions associated with technologies

Figure 29 presents a Venn diagram associating the SENTINEL value propositions with technologies. The technologies that have been developed and enhanced in the context of SENTINEL as a result of the technical development conducted in the entire project period are represented with the SENTINEL logo, while external ones appear with a diamond legend.

The core functionalities of SENTINEL include:

- The GDPR Compliance Self-Assessment Engine that performs intelligent requirement analysis to assess the PDP risk and calculate the Risk Assessment for Small Enterprises (RASE) score and Company profile which populates the SME profiles and provides persistence for storing and fetching organisation and Processing Activity (PA) data.
- The Recommendation Engine, for automated but informed plugin recommendations based the participants needs as captured by the RASE score as well as their budgetary and resource allocation constraints
- The Policy Drafting Engine that enhances the plugin recommendations with related trainings (via recommendation service of open-source tools/courses) and drafts a comprehensive security policy for the SME
- The Incident Reporting and Sharing module that helps inform regulators, security teams and other external bodies about potential incidents in a structured manner
- The Observatory Knowledge Base and the Information Exchange module, that enable the exchange of critical data and knowledge over threats, signatures and evidence as well as anonymised policy drafts between the SME and open security data sharing platforms

The SENTINEL internal plugins and external plugins/trainings are:

- ***GDPR Compliance Self-Assessment (GDPR CSA)*:** GDPR CSA is designed to support SMEs/MEs to be accountable regarding the processing of personal data by helping them to identify what are the requirements to meet to process personal data, check that Organisational or Technical Measures (OTMs), and identify what and how to improve accountability.
- ***Security Infusion (SI):*** SI offers holistic IT event management and cybersecurity risk mitigation. It is used as part of the "Receive Security Notifications" use case. Agents can be installed on the premises of one of the SENTINEL partners and monitor pre-determined parts of its infrastructure.
- ***Identity Management System (IdMS):*** It delivers a solution that enables the creation of centralized, trusted digital identities for individuals, relates these identities with specific roles and access rights, and finally uses these identities to securely leverage both user data and SME data, so SENTINEL participants may be GDPR compliant in terms of data portability and data sovereignty.
- ***MITIGATE*:** Offers multi-order and impact assessment capabilities for identifying/assessing risks, threats and incidents and estimates their impact in interdependent infrastructures. It promotes collaboration among business entities in assessing and exploring their risks allowing them to manage their cybersecurity in a holistic and cost-effective manner.
- ***Data Privacy Impact Assessment (DPIA):*** It provides the capability to execute data protection impact self-assessments and is designed to allow SMEs to identify (through assessment) and minimise (through recommendations) the risks associated with their personal data processing activities. DPIA is demarcated as mandatory for Processing Activities which are likely to result in high risks to individuals' data privacy
- ***CyberRange***: provides gaming interface by focusing on training and educational content to raise awareness to the SME's best practice, for data protection and GDPR. The CyberRange gaming interface gives SME's the ability to test, evaluate, and train in real-world cyber threat scenarios.
- ***Forensics Visualisation Toolkit (FVT):*** offers a complete toolset for IT security data collection, processing, and visualization.
- **External Plugins and Trainings:** the SENTINEL platform can also suggest to the user 54 external free/open-source tools and 117 training components to fill the identified gaps. These solutions cover all the OTM capabilities that are subject to the SENTINEL methodology.

6. Business Model

This section is about investigating the potential systematic ways for SENTINEL to unlock long-term value for the project outcome after the project's end, while delivering valuable products and services. The business model, according to the author of the Business Model Canvas [21], "describes the reasoning of how an organization develops, delivers, and collects value."

A preliminary business model canvas of the project has already been established in M6 and reported in D7.2 "Market analysis & preliminary business modelling". There, all nine building blocks/elements of the canvas have been presented and thoroughly analysed. Additionally, a complementary canvas has been included in D7.7 "Exploitation strategy, standardisation activities & best practices - interim version", where we have presented the updates achieved, as a result of our study conducted for each element of the canvas since M6.

In this section, we describe the final business model of the SENTINEL project and perform a techno-economic analysis to evaluate its sustainability. In particular, we run a discounted cash flow analysis and compute financial figures like the Return on Investment (ROI), net-present value (NPV), sales figures and alike. We also perform a sensitivity analysis on the key parameters driving the cost items and revenue streams.

6.1 Business model characterization

According to the Business Model Canvas idea, a business model consists of nine basic parts that demonstrate the logic of increasing profit for the organization. These are summarized in Figure 30 and described in detail in the sections below.

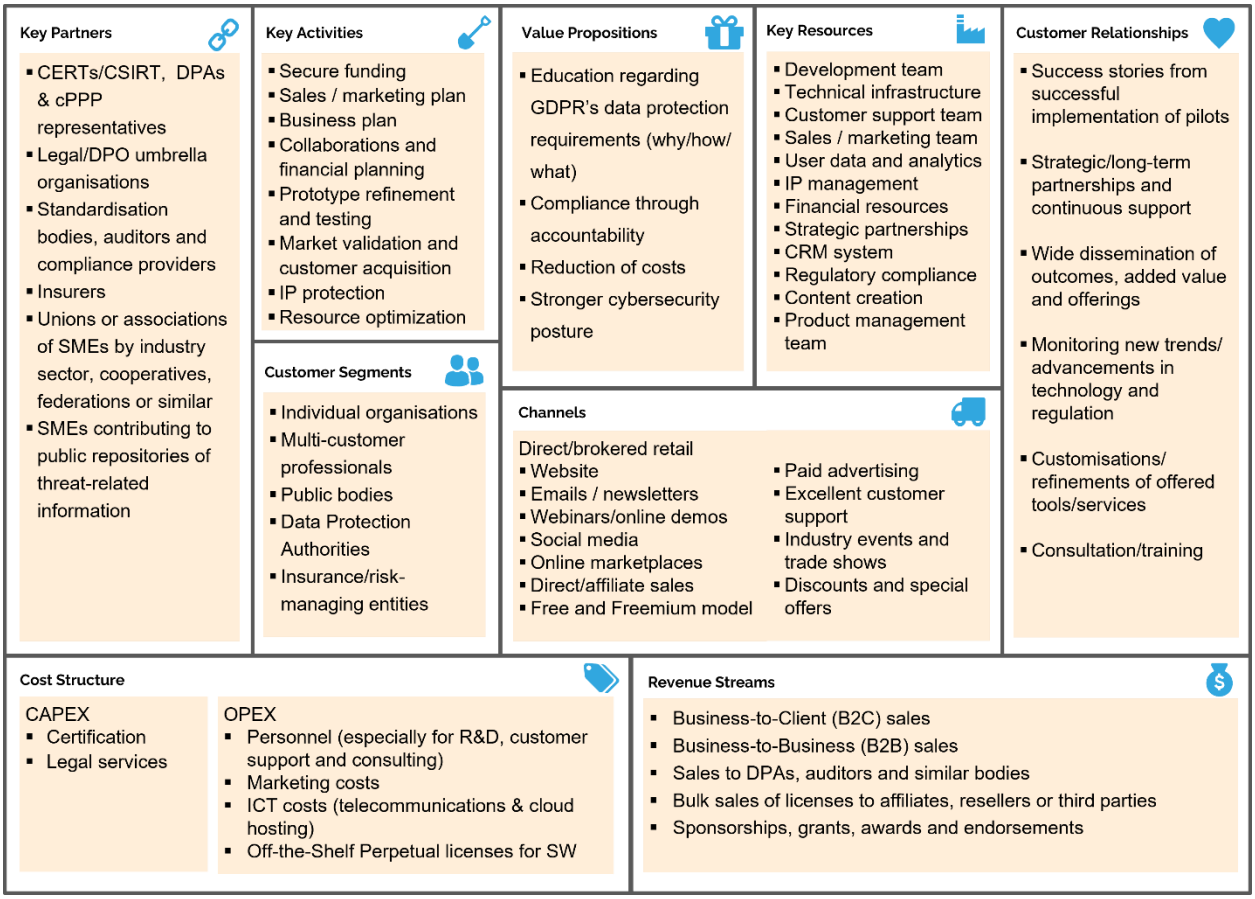

Figure 30. Final SENTINEL Business Model Canvas

6.1.1 Customer segments

SENTINEL primarily addresses SMEs of all industries in Europe, and worldwide, but does not exclude larger enterprises, public authorities or any organisation which processes personal data. The SENTINEL customer profile is organisations who need to address data protection compliance but lack the resources to completely outsource it. Specifically, SENTINEL is intended for:

(a) **Individual organisations**, to be used by i) executives with a high-level decision making capacity on the organisation's data processing activities, such as directors, CEOs, CTOs or similar, as well as ii) employees looking to better understand the nature and GDPR compliance level of the data processing and acquire recommendations, as well as improve their cybersecurity and data protection practices, and iii) Technical/IT personnel at any level, tasked with maintaining cyber assets and/or implementing technical measures for data protection;

(b) as a **B2B** offering for data protection professionals (lawyers, law firms and DPOs) working with multiple customers;

(c) **public bodies** of any scale and level, looking to improve their own data protection practices;

(d) **national or regional data protection authorities** (e.g. DPAs) looking for software to help them to execute compliance assessments for candidate organisations;

(e) **Insurance companies and risk-managing entities** looking to assess the risk and compliance level associated with their customers' data protection practices.

6.1.2 Value proposition

SENTINEL offers customers a quadruple value proposition:

(a) To **educate** themselves about GDPR's data protection requirements and, specifically, why individuals' data and privacy need protection, how the personal data processing activities may affect data subjects' privacy, and what needs to be done in terms of organisational and technical measures (what GDPR refers to as the security of personal data), complemented with training and educational material for cybersecurity, data protection and privacy.

(b) To **achieve compliance through accountability** by documenting (keeping records of) their processing activities as well as evidence supporting their GDPR compliance claims. Specifically, SENTINEL offers: a Record of Processing Activities (ROPA) to help businesses comply with Art.30 of the GDPR for keeping records of how personal data is processed and the nature and intention of data processing activities, as well as and a mapping between the identified data protection requirements and the specific recommended organisational and technical measures, training material and software & tools to satisfy them.

(c) To **reduce costs** by automating key data protection compliance processes, generating intelligent recommendations of measures, tools and trainings and overall acquainting key business and technical people in the organisation with data protection compliance principles, thus saving on consultancy, training and education costs. As an example, an SME stakeholder, after having completed a SENTINEL user journey, will have a more holistic understanding of the EU's data protection requirements, their own organisation's GDPR compliance assessment, the estimated risk associated with their Processing Activities and organisation as a whole and what specific measures need to be put in place to strengthen their compliance and their whole privacy and security stance.

(d) To **strengthen their cybersecurity** through enterprise-grade and well-integrated tools, adapted for smaller businesses, such as the Airbus CyberRange and Mitigate.

6.1.3 Channels

The **channels** describe how a company reaches its customers to deliver value. An effective channel strategy will distribute a company's value proposition in ways that are fast, efficient and cost-effective. An organization can reach its customers either through physical channels (e.g. POP, store front, etc), digital channels, B2B and channel partners (distributors), or a combination. In SENTINEL, we envision two different categories of channels: (a) direct retail (especially towards SMEs) and (b) brokered retail (via SMEs associations that will act as intermediaries to market, promote, and deliver product subscriptions to their members). Table 8 presents more details about each one.

Table 8. SENTINEL sales channels

Direct retail
Product website: The main online presence of the platform, where potential customers can learn about it, sign up for a subscription, and access the service. This option offers full control

over branding, user experience, and customer data. Furthermore, it serves as the central hub for product information, demos, and customer support.
Email/newsletter marketing: Email campaigns that inform customers about new features, offer promotions, and share educational content. This option offers direct, personalized and cost-effective communication with targeted messaging.
Webinars and online demos: Hosting live or recorded webinars and product demos to showcase the platform's features and benefits. This option provides an interactive way to educate potential customers, build trust, and address questions and concerns directly.
Social media platforms: Utilizing platforms like LinkedIn, X, Facebook, and YouTube to promote the product, share updates, and engage with users. This option offers broad reach, enhances brand visibility, and allows for targeted advertising and community building.
Content marketing: Creating and distributing valuable content such as blogs, whitepapers, case studies, and video tutorials to attract and retain customers. This option establishes authority and trust and educates customers about the product's value.
Online marketplaces: Listing the service on platforms like AWS Marketplace, Microsoft Azure Marketplace, and Google Cloud Marketplace. This option increases visibility and provides customer reviews and ratings.
Affiliate marketing: Partnering with third-party websites/promoters to promote the product in exchange for a commission on sales. This option expands reach through trusted recommendations, performance-based cost, and enhances brand credibility.
Free and Freemium model: Offering a limited free or a more inclusive freemium version of the product to allow potential customers to experience the product before committing to a subscription. This option presents a low barrier to entry, increases user adoption, and allows users to experience value firsthand before purchasing.
Paid advertising: Utilizing online advertising channels such as Google Ads, Facebook Ads, and LinkedIn Ads to target potential customers. This approach offers targeted reach, measurable results, and the ability to quickly scale efforts based on performance.
Customer support and onboarding: Providing excellent customer support and comprehensive onboarding to ensure customers get the most out of the platform. This approach increases customer satisfaction and retention, reduces subscription cancelations/non-renewals, and encourages word-of-mouth referrals to new customers.
Industry events and trade fairs: Participating in industry-specific events and trade shows to showcase the platform to a targeted audience. This approach offers direct interaction with potential customers, opportunity for live demonstrations, and building industry connections.
Brokered retail
SMEs association websites: The main online platform where members can learn about the product, be redirected to the product website and access the service. This approach offers a centralized and trusted source of information, high traffic from association members, and direct access to target audience.
Email newsletters: Regular email updates sent by the association to its members, featuring information about the product, promotions, and educational content. This approach offers direct and personalized communication, high message open rates due to trust in the association, and cost-effective marketing.
Webinars and online workshops: Hosting live or recorded webinars and workshops to demonstrate the platform's features and benefits to association members. This approach offers interactive and engaging way to educate potential customers, build trust, and address questions and concerns directly.

Social media channels: Utilizing the association's social media platforms like LinkedIn, X, Facebook, and YouTube to promote the product and share updates. This approach offers broad reach, enhances visibility, and allows for targeted advertising and community engagement.
Direct sales through association representatives: Employing a sales team within the association to engage directly with members, especially for tailored solutions and enterprise-level subscriptions. This option offers personalized sales approaches, ability to handle complex sales processes, and builds strong customer relationships.
Partnering with educational and training programs: Integrating the product into the association's educational programs and training workshops for its members. This option offers increased adoption among association members, brand visibility in educational contexts, and long-term customer relationships.
Association events and member meetings: Showcasing the platform at regular association events, member meetings, and networking sessions. This option offers direct engagement with potential customers, opportunity to provide live demonstrations, and foster a sense of community around the product.
Online forums and member communities: Leveraging online forums and member communities hosted by the association to discuss the product and share user experiences. This approach facilitates peer-to-peer recommendations, provides a platform for addressing questions and concerns, and builds a user community.
Discounts and special offers for members: Offering exclusive discounts and special offers on the subscription for association members. This approach incentivizes adoption, rewards membership loyalty, and provides a competitive advantage.

6.1.4 Customer relationship management

SENTINEL aims to build its customer relationships through presenting success stories from successful implementation of pilots and through strategic partnerships to reach the broader dissemination and exploitation channels possible. It aims to ensure long-term relationships by providing continuous support to evolving requirements of each targeted domain, by monitoring the new trends arising and the advancements in technology and regulation domain. Moreover, we seek to build upon customizations and refinements in order to meet the emerging resource provisioning needs of customers, offering consultation and training as well.

6.1.5 Revenue streams

There is a high potential to create sources of revenue by directly selling the SENTINEL platform. To promote the framework and engage new users and early adopters, a basic and restricted version of the platform can be offered free-of-charge following the Freemium model[43]. The targeted audience can be:

(a) Business-to-Client (B2C): Directs sales of SaaS recurring annual licenses to entities managing one organisation (per seat)
(b) Business-to-Business (B2B): Direct sales of SaaS recurring annual licenses to entities managing other organisations (multi-organisation, with collaboration features)

[43] Note that the SENTINEL platform shall benefit from those customers to contribute anonymous information to the SENTINEL Observatory

(c) DPAs, auditors and similar bodies: Direct sales of SaaS recurring annual licenses to entities auditing and/or assessing other organisations (multi-organisation, with collaboration features)
(d) Bulk / wholesale sales of licenses to affiliates, resellers or third parties
(e) Sponsorships, grants, awards and endorsements

The SENTINEL pricing strategy and revenue streams scenarios are illustrated in Sections 6.2 and 6.3 in more detail.

6.1.6 Key resources

Here, we identify the most important assets required to make the SENTINEL business model work. The human and financial capital are at the top of the list, as they will drive business success. Furthermore, strong partnerships with the European research community and industry are essential. Table 9 provides more details regarding the key resources we identified for SENTINEL.

Table 9. SENTINEL key resources

Key resources
Software development team: Skilled developers, designers, and engineers. These are essential for maintaining, updating, and improving the platform to meet customer needs and stay competitive.
Technical infrastructure: Servers, databases, cloud services, and other IT infrastructure needed to host and run the platform. These are critical for ensuring reliable, scalable, and secure service delivery to customers.
Customer support team: Support staff and resources dedicated to assisting customers with issues, questions, and onboarding. These are important for maintaining high customer satisfaction, retention, and successful onboarding experiences.
Sales and marketing team: Professionals focused on acquiring new customers, retaining existing ones, and promoting the product. These are vital for driving growth, increasing market presence, and managing customer relationships.
User data and analytics: Systems and tools for collecting, analyzing, and leveraging user data to improve the platform and customer experience. These enable data-driven decision-making, personalization, and continuous improvement of the platform.
Intellectual property management: Patents, trademarks, and proprietary technologies that protect the platform and its unique features. These provide competitive advantage and protect the product from infringement.
Financial resources: Capital and financial assets needed for operational expenses, marketing, and strategic investments. These ensure the SENTINEL joint team can sustain operations, scale, and invest in growth opportunities.
Strategic partnerships: Relationships with other companies, platforms, organizations and communities that enhance the platform's value proposition. They provide additional features, integrations, and market reach that can boost the platform's appeal and functionality.
Customer relationship management (CRM) system: They are tools and platforms for managing interactions with current and potential customers.
Legal and regulatory compliance: Legal expertise and systems to ensure compliance with data protection, privacy laws, and other regulations. It protects the partnership from legal risks and ensures customer trust and confidence.

Content creation resources: Teams and tools for creating educational content, marketing materials, and support documentation. There are essential for marketing, customer education, and providing comprehensive support resources
Product management team: Product managers who oversee the platform maintenance/update lifecycle and ensure alignment with market needs and business goals. They are critical for prioritizing features, guiding development, and aligning the product with customer demands and business strategy.

6.1.7 Key activities

Beyond the project, our aim will be to continue a number of activities started during the project, by seeking potential investors and approaching early adopters. In this regard, we have envisioned a number of indicative activities that are summarised below. More details can be found in D7.8 "Exploitation strategy, standardisation activities and best practices - final version" and specifically in Section 4.1.5.

(a) Securing funding.
(b) Drafting and implementing a sales and marketing plan.
(c) Finalising the business plan.
(d) Collaborations and financial planning.
(e) Prototype refinement and testing.
(f) Market validation and customer acquisition.
(g) Intellectual property protection.
(h) Resource optimization

By focusing on securing funding and implementing a robust sales and marketing plan, the project aims to achieve a successful market launch, while supporting secondary activities to enhance overall readiness and sustainability.

6.1.8 Key partnerships

From a business perspective, the wide adoption of our offerings requires effective standardization efforts and partnerships with CERTs/CSIRT, DPAs and cPPP. The project's partners satisfy all the categories needed from research and industry community in various sectors. Furthermore, SMEs contributing to the SENTINEL Knowledge Base or other public repositories of threat-related information (that SENTINEL Observatory is connected to) are considered key supporters of our vision. Key players who would activate our channels and/or revenue streams include, but are not limited to:

(a) Legal/DPO umbrella organisations
(b) Standardisation bodies, auditors and compliance providers
(c) Insurers
(d) Unions or associations of SMEs by industry sector, cooperatives, federations or similar

6.1.9 Cost structure

Cost items are usually organised either as capital or operational expenditures, also known as CAPEX and OPEX, respectively. CAPEX refers to long-term expenses for acquiring tangible assets (e.g., equipment) and intangible ones (e.g., software or services). These costs can be

recurring as well, e.g., when they refer to upgrading and maintaining those assets. On the other hand, OPEX refers to ongoing/recurring costs that a software/service provider must spend to realise its offering. In contrast to capital expenditures, whose lifetime extends beyond the accounting period of the actual spend, the benefits derived from operational expenses are exhausted within the same accounting period/year and are not carried after that. The cost structure of the SENTINEL platform is illustrated in Section 6.2 in more detail.

6.2 The SENTINEL cost model

A key part of an entity's business model refers to defining its cost structure, i.e., the capital and operating expenditures, as well as their evolution over time.

6.2.1 Capital expenditures

While Capital Expenditures (CapEx) may involve several categories, such as those for Software acquisition (e.g., buying one-time off-the-Shelf software licenses), Information & Communications Technology (ICT) equipment like servers, workstations, routers, etc., in SENTINEL we focus on costs related to Services. In particular, we focus on the following ones:

- Certification costs: Cost for getting certificates from international organisations that the individual SENTINEL modules comply with industry standards. Obtaining certificates from recognized bodies is considered to be an investment, as it demonstrates the consortium's commitment to complying with cybersecurity and data protection best-practices (e.g., ISO/IEC 27001:2022) and regulations (e.g., GDPR). This can boost customer confidence of choosing a long-lasting and trustworthy solution, and make sure that SENTINEL keeps up with established competitors while gaining competitive advantage over newcomers. We shall assume that the certification cost for each module is 3000 € and lasts for 6 years.
- Legal services: Involving legal experts is key for compiling Terms-of-Use for the SENTINEL platform and preparing a clear and concise SENTINEL Joint Exploitation agreement to be signed by all interested consortium members. We assume that such documents will be based on well-defined templates and thus a moderate cost of 1000 € has been considered in the calculation of financial metrics of Section 6.4.

6.2.2 Operating expenditures

The SENTINEL Operating Expenditures (OpEx) include several categories and cost items, which are presented below:

6.2.2.1 Salaries

- Junior Employee Salaries: Junior Employee Salaries Costs, especially for SW developers, Marketing staff, Sales staff and Admin staff. In particular, we assume that the average salary for a Full Time Equivalent (FTE) of a junior employee is 24000 € and that in the context of SENTINEL, each partner engages a portion of their working hours as follows:
    - Engineer: 20% of an FTE for making updates to the respective module(s)
    - Marketing staff: 5% of an FTE for running marketing campaigns
    - Sales staff: 20% of an FTE for contacting customers

- Admin staff: 5% of an FTE for handling the rest of the activities.

- Senior Employee Salaries: Senior Employee Salaries Costs especially for system architects, as well as senior salespersons. We assume that a full-employed senior member receives 40000 € on average and that each SENTINEL partner engages 9,0% of an FTE for each of these two employee types.

- Manager Salaries: Manager Salaries Costs, especially for involving executive members. We assume that the average manager salary is 60000€ for an FTE and that each partner involves the following positions:

  - 3% of the Chief Executive Officer (CEO)
  - 3% of the Chief Technology Officer (CTO)
  - 3% of the Chief Financial Officer (CFO)
  - 3% of the Chief Communications Officer (CCO)

6.2.2.2 Customer Support

Call center members are important for assisting customers' users when they cannot complete a task, despite the availability of clear documentation. We assume a 3-tier customer support structure in order to better serve the different types of SENTINEL customer base [43]. Tier 1 agents are typically trained to efficiently address frequent problems, which leads to improved First Contact Resolution (FCR) rates at a lower cost. In particular, we assume that 20% of calls to Tier 1 personnel are unresolved and consequently escalate to the next level, involving more senior employees. Similarly, 20% of sessions handled by Tier-2 representatives will eventually need to involve Tier-3 members, who can deal with extreme cases. Apart from efficiency, high FCR rates means that customers' questions are effectively handled, leading to higher customer satisfaction. Such a multi-tier service model not only allows us to efficiently and effectively assist the SENTINEL customer base, but also to increase attractiveness of premium offers. In particular, we assume that Premium and B2B customers skip the Tier-1 customer support and are directly connected to 2nd level. Furthermore, the average customer service time per session is 12 minutes regardless of customer type, while we assume that Free users can contact the call center only once.

The salary of customer support members is as follows:

- 24000€ for Tier-1
- 28000€ for Tier-2
- 32000€ for Tier-3

6.2.2.3 ICT costs

- Cloud hosting costs: Costs for renting the infrastructure where the SENTINEL integrated platform and/or its external plugins can be hosted. All the SENTINEL tools and services are taken into consideration in our assumption and thus the Cloud hosting costs comprise the following VMs/containers:

- CyberRange
- GDPR CSA
- DPIA
- MITIGATE
- Security Infusion
- SENTINEL, which includes the User Interface and the Observatory
- SENTINEL Common Backend, which contains the Identity Management System, the API Gateway, the Orchestrator service, the Message Broker and the Plugins Service
- CICD, acting as a development server.

By making assumptions on the average number of user sessions per customer per module per year and the average execution hours per session per module, we were able to compute the yearly load per module. Then, by making assumptions on the number of vCPUs per type of server employed, we were able to calculate the number of instances needed for each year. Based on the price per server per hour, we were able to compute to annual costs per server type.

- Other ICT costs (e.g., Internet connectivity) were assumed to be 5000 € annually.

6.2.2.4 Software

- SW Licence Renewal Costs: Costs for renewing SW licenses (for the software that is not one-time) were assumed to be 7500€ per year.

6.2.2.5 Customer acquisition and maintenance

- Advertisement Costs: Costs for dissemination and communication involved:
  - 10000€ for events
  - 15000€ for online advertisements, brochures, etc.

6.2.2.6 Consulting

- Legal Consulting Costs: Cost for getting advice from external legal experts.

6.3 Revenue streams

We have defined five pricing plans for the SENTINEL platform, as listed in Table 10.

Table 10. SENTINEL pricing plans and capabilities available

Pricing plan	Description	Capabilities available
Free	Time trial, limited access to basic features. Auto reverts to Standard after trial period expires, unless cancelled	• Single organisation • 1 processing activity • <10 assets • 1 GDPR Compliance Self-Assessment • 1 DPIA • 1 Cybersecurity assessment (CSRA)

		• 14-day limit
Freemium	Time trial, unlimited access to some activated basic features. Auto reverts to Standard after trial period expires, unless cancelled	If GDPR CSA was activated: • Single organisation • Unlimited processing activities • Unlimited assets • Unlimited GDPR Compliance Self-Assessments • 1 Data Protection Impact Assessment • 1 Cybersecurity risk assessment • 14-day limit
Standard	Unlimited access to all basic features	• Single organisation • Unlimited processing activities • Unlimited assets • Unlimited GDPR Compliance Self-Assessments • Unlimited Data Protection Impact Assessments • Unlimited Cybersecurity risk assessments
Premium	Unlimited access to all features for a single organisation	• Single organisation • Unlimited processing activities • Unlimited assets • Unlimited GDPR Compliance Self-Assessments • Unlimited Data Protection Impact Assessments • Unlimited Cybersecurity risk assessments • Access to the Cyber Range • Incident handling • Threat Intelligence feeds
B2B	Unlimited access to all features for multiple organisations	

Having outlined these pricing plans, we can proceed with the definition of the following annual revenue streams:

Table 11. Calculation method of annual revenue streams

Pricing plan	Calculated as
Freemium	"Average SENTINTEL Add-on monthly price" x 12 Months x "Number of Freemium customers" x "Average number of add-ons activated per Freemium customer" x "probability of >=1 add-ons activated per Freemium customer
Standard	"STANDARD SENTINEL plan monthly price" x 12 Months x "Number of standard customers
Premium	"PREMIUM SENTINEL plan monthly price" x 12 Months x "Number of premium customers"
B2B	"B2B SENTINEL plan monthly price" x 12 Months x "Number of B2B customers"

6.4 Financial analysis

6.4.1 Financial analysis of baseline scenario

In the following, we perform a financial analysis of SENTINEL joint exploitation scheme, for a 5-year period in the baseline scenario.

Table 12 presents the estimated revenue streams at the end of Year-1, as computed based on the assumptions employed to each revenue stream driver in the baseline scenario. These assumptions refer to the figure of each revenue driver, as well as the annual increase rate considered.

Table 12. Revenue streams estimation in Year-1

Revenue Stream	Revenue driver figure	Comments	Annual increase rate
Annual revenues from STANDARD SENTINEL plan	34800	Computed automatically as the product of the 3 revenue stream drivers below	
STANDARD SENTINEL plan monthly price	29	Based on "penetration pricing" strategy	0% (fixed)
Number of standard customers	100	Based on assumptions	100%
Number of months	12	Based on assumptions (0% customer attrition rate)	N/A
Annual revenues from PREMIUM SENTINEL plan	21240	Computed automatically as the product of the 3 revenue stream drivers below	
PREMIUM SENTINEL plan monthly price	59	Based on "penetration pricing" strategy	0% (fixed)
Number of premium customers	30	Based on assumptions	100%
Number of months	12	Based on assumptions (0% customer attrition rate)	N/A
Annual revenues from B2B SENTINEL plan	3588	Computed automatically as the product of the 3 revenue stream drivers below	
B2B SENTINEL plan monthly price	299	Based on "penetration pricing" strategy	0% (fixed)
Number of B2B customers	1	Based on assumptions	100%
Number of months	12	Based on assumptions (0% customer attrition rate)	N/A
Annual revenues from FREEMIUM plan	45000	Computed automatically as the product of the 5 revenue stream drivers below	

Average SENTINEL Add-on monthly price	15	Based on "penetration pricing" strategy	0% (fixed)
Number of FREEmium customers	2500	Based on assumptions	100%
number of add-ons activated per FREEmium customer	1	Based on assumptions	0% (fixed)
probability of >=1 add-ons activated per FREEmium customer	10%	Based on assumptions	0% (fixed)
Number of months	12	Based on assumptions (0% customer attrition rate)	N/A

Table 13 presents how the number of customers for each of the 4 segments evolves over the 5-year period assuming a 100% annual increase rate (as the baseline scenario).

Table 13. Evolution of the number of customers per segment over the 5-year period in the baseline scenario

	Year 1	Year 2	Year 3	Year 4	Year 5
Pricing plan	**# of Customers**				
Freemium	2500	5000	10000	20000	40000
Standard	100	200	400	800	1600
Premium	30	60	120	240	480
B2B	1	2	4	8	16

Furthermore, Table 14 presents how each of the 4 revenue streams contribute to the total income of SENTINEL joint exploitation scheme.

Table 14. Estimated revenues for SENTINEL joint exploitation scheme in the baseline scenario over a 5-year period

	Year					
Revenue Stream	**0**	**1**	**2**	**3**	**4**	**5**
Monthly revenues from STANDARD SENTINEL plan	0	34.800	69.600	139.200	278.400	556.800
Monthly revenues from PREMIUM SENTINEL plan	0	21.240	42.480	84.960	169.920	339.840
Monthly revenues from B2B SENTINEL plan	0	3.588	7.176	14.352	28.704	57.408
Monthly revenues from FREEMIUM plan	0	45.000	90.000	180.000	360.000	720.000
Total Revenues	**0**	**104.628**	**209.256**	**418.512**	**837.024**	**1.674.048**

As evidenced from Table 15, we follow a "penetration" pricing policy by announcing an annual license fee of 348€/year for the Standard plan, which is similar to the price asked by GDPR

Manager (i.e., the solution offering the closest service portfolio at the most competitive price) or 18% higher compared to GDPRWise that offers limited functionality (GDPR self-assessment alone). When it comes to the premium pricing plan, it involves an annual license fee of 708€/year, which is about 2% the annual fees asked by OneTrust Pro for a similar configuration that does not include CyberRange functionality.

Table 15. Prices of competing tools

Tool name	Annual license fee (excluding VAT)	Comments
OneTrust Pro	37860 €/year	Annual license fee[44] for similar service portfolio excluding CyberRange, broken down as follows: • 5227€/year for DPIA, • 5227€/year for Incident Handling, • 5460€/year for GDPR & Policy • management, • 16200 €/year for CSRA
GDPR Manager	350 €/year	Annual license fee[45] for CyberComply tool that offers DPIA, Incident Manager, GDPR Compliance Manager tool, Risk manager
GDPRWise	295 €/year	Annual license fee[46] for GDPR self-assessment for an EU-based SMEs
SENTINEL Standard	**348 €/year**	**Annual license fee for Standard plan**
SENTINEL Premium	**708 €/year**	**Annual license fee for Premium plan**

Table 16 summarizes our assumptions on the capital expenditures of the SENTINEL consortium in the baseline scenario, i.e., the third-party services to be purchased before SENTINEL is being launched but used for several years (as shown in "Renewal every (years)" column). For example, assuming that the certificate for each of the 9 modules costs 3000€ and is renewed every 6 years, then certification costs are estimated at 27000€ for the 5-year evaluation period.

Table 16. Capital expenditures for baseline scenario

Capital Expenditure	Unit	Cost figure	Renewal every (years)	Comments
Certification Fees	€/year	27000	6	9 certificates to be issued; each one costs 3000€. A Certificate is assumed to last for 6 years.
Legal services	€/year	1000	10	A legal expert prepares the Terms of Service and the Joint exploitation agreement.

[44] Based on pricing information available online at https://web.archive.org/web/20240314074646/ https:/www.onetrustpro.com/buy/
[45] Based on pricing information available online at https://www.vigilantsoftware.co.uk/product/cybercomply
[46] Based on pricing information available online at https://gdprwise.eu/pricing/

When it comes to operating expenditures, Table 17 presents the annual expenses, along with the assumed annual increase rate. Furthermore, a brief justification on the cost figures appears in the "Comments" column.

Table 17. Operating expenditures

Operating Expenditure	Unit	Cost figure	Annual increase rate	Comments
Customer support for Free customers	€/year	3885,45	100%	Cost figure based on simulation results (see Table 18 and related discussion for more details). Increase rate based on assumption on increase rate of Free customers.
Customer support for Freemium customers	€/year	1400,21	100%	Cost figure based on simulation results (see Table 18 and related discussion for more details). Increase rate based on assumption on increase rate of Freemium customers.
Customer support for Standard plan customers	€/year	1683,13	100%	Cost figure based on simulation results (see Table 18 and related discussion for more details). Increase rate based on assumption on increase rate of customers adopting Standard plan.
Customer support for Premium customers	€/year	1443,36	100%	Cost figure based on simulation results (see Table 18 and related discussion for more details). Increase rate based on assumption on increase rate of premium customers.
Customer support for B2B customers	€/year	64,15	100%	Cost figure based on simulation results (see Table 18 and related discussion for more details). Increase rate based on assumption on increase rate of B2B customers.
Full-time equivalent (FTE) for managers	FTE/month	108%	0%	FTE figure based on simulation results. Increase rate based on assumption of 0% inflation.
Annual salary (average) for managers	€/year	60000 €	0%	Figures based on assumptions.
Full-time equivalent (FTE) for senior employees	FTE/month	162%	0%	FTE figure based on simulation results. Increase rate based on assumption of 0% inflation.

Annual salary (average) for senior employees	€/year	40000 €	0%	Figures based on assumptions.
Full-time equivalent (FTE) for junior employees	FTE/month	450%	0%	FTE figure based on simulation results. Increase rate based on assumption of 0% inflation.
Annual salary (average) for junior employees	€/year	24000 €	0%	Figures based on assumptions.
SW Licence Renewal Costs	€/year	7500	0%	Figures based on assumptions.
Other ICT Costs	€/year	5000	20%	Figures based on assumptions.
Dissemination & Communication Costs	€/year	25000	0%	Figures based on assumptions.
Cost for renting GDPR cloud server	€/year	1409,4	72%	Figures based on assumptions.
Cost for renting CyberRange cloud server	€/year	1409,4	72%	Figures based on simulation results taking into account customer mix evolution.
Cost for renting MITIGATE cloud server	€/year	939,6	72%	Figures based on simulation results taking into account customer mix evolution.
Cost for renting SecurityInfusion cloud server	€/year	469,8	72%	Figures based on simulation results taking into account customer mix evolution.
Cost for renting DPIA cloud server	€/year	1409,4	72%	Figures based on simulation results taking into account customer mix evolution.
Cost for renting OTHER_EXTERNAL cloud server	€/year	0	72%	Figures based on simulation results taking into account customer mix evolution.
Cost for renting CICD cloud server	€/year	359,88	72%	Figures based on simulation results taking into account customer mix evolution.
Cost for renting SENTINEL Backend cloud server	€/year	469,8	72%	Figures based on simulation results taking into account customer mix evolution.
Cost for renting SENTINEL Common Backend cloud server	€/year	469,8	72%	Figures based on simulation results taking into account customer mix evolution.
Cost for Legal advices	€/year	15000	0%	Figures based on assumptions.

In order to estimate costs associated with the customer support scheme described in 6.2.2.2, we had to make assumptions on the annual number of requests per customer type reaching the designated customer support level (e.g., Premium and B2B reaching Tier-2 directly), the percentage of requests that escalate to the next level (i.e., 20%), the mean service time (i.e., 12 minutes) and the number of customers belonging to each group. Table 18 presents the FTEs

required per customer representative type (rows) in order to serve different each type of customer in Year-1. For the subsequent years, we assumed that the cost for handling each customer type scales up according to the annual increase rate of that customer segment.

Table 18. The estimated effort on call center representatives by each type of user

	Free	Freemium	Standard	Premium	B2B	Total FTEs needed per Tier
Tier-1 FTEs	16,1875%	5,8275%	6,9930%	0%	0%	29,0080%
Tier-2 FTEs	0,0013%	0,0047%	0,0140%	4,1958%	0,1865%	4,4022%
Tier-3 FTEs	0,0003%	0,0009%	0,0028%	0,8392%	0,0373%	0,8804%

To conduct the financial analysis, we assume that:

- Prices are assumed to be static,
- the interest rate used for discounting future cashflows (revenues or expenses) is 1%,
- Corporate Tax Rate is 22%.

The following figure shows the Evolution of Free Cash Flows for the SENTINEL joint exploitation. We observe that the payback period is in year 4 and the total profit is approximately EUR 1,354 Mn.

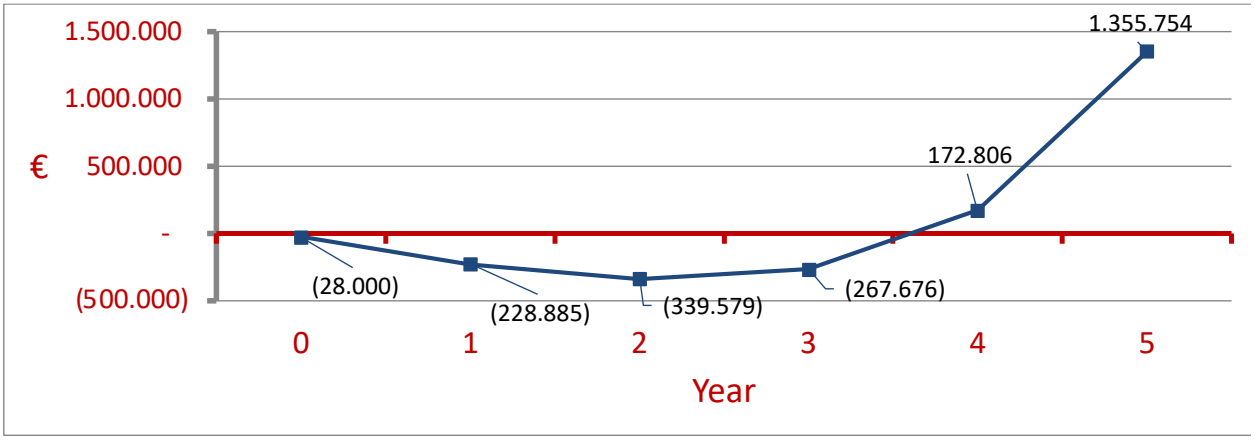

Figure 31. The evolution of Free Cash Flows for the SENTINEL joint exploitation scheme in the baseline scenario over a 5-year period

After performing a discounted cash flow analysis, we are able to compute the following financial key performance indicators:

- **Internal Rate of Return (IRR):** represents the rate that makes the present value of all revenues associated with a business model equal to the present value of all expenses. Higher IRRs are generally considered more attractive, as they indicate a higher potential for returns.

- **Present Value of Free Cash Flow (FCF):** represents the cash that is available for distribution to investors, debt reduction, or reinvestment in the business, discounted at a specific discount rate to reflect the time value of money.
- **Present Value of CAPEX**: represents the current value of the capital expenditures by discounting all capital expenses at the selected discount rate.
- **Present Value of OPEX**: represents the current value of the operating expenditures by discounting all running expenses at the selected discount rate.
- **Present Value of Revenues**: represents the current value of the revenues by discounting these at the selected discount rate.
- **Return on Investment (ROI)**: represents the expected return obtained from a business model relative to its cost.
- **Payback period**: represents the number of years it takes for a business model to generate cash inflows sufficient to recover its initial cost.

Table 19. Key financial metrics for SENTINEL joint exploitation scheme in the baseline scenario over a 5-year period

Internal Rate of Return (IRR)	49%
Return on Investment (ROI)	921.449
Present Value of FCF	28.000
Present Value of CAPEX	1.800.883
Present Value of OPEX	3.112.091
Present Value of Revenues	70%
Payback period	4

6.4.2 Financial analysis of alternative scenarios

Apart from the baseline scenario described in 6.4.1, we analysed a number of alternative scenarios with respect to expected demand conditions, as shown in Table 20. These conditions reflect the uncertainty about the number of customers (regardless of their type) attracted in Year 1 and the annual increase rate in customer acquisition. The 9 scenarios (including the baseline one) can be grouped as follows:

- “pessimistic” ones that include the red-coloured cases (i.e., “Very Pessimistic Scenario”, the “Pessimistic Scenario 1” and “Pessimistic Scenario 2”).
- Optimistic ones that include the green-coloured cases (i.e., “Very Optimistic Scenario”, the “Optimistic Scenario 1” and “Optimistic Scenario 2”).
- Uncertain ones, that include the yellow-coloured cases.

Table 20. Description of market scenarios analysed

		Customer annual increase rate		
		80%	**100%**	**120%**
Y1 number of customers (compared to baseline)	**80%**	Very Pessimistic Scenario	Pessimistic Scenario 2	Uncertain Scenario 2
	100%	Pessimistic Scenario 1	Baseline Scenario	Optimistic Scenario 2
	120%	Uncertain Scenario1	Optimistic Scenario 1	Very Optimistic Scenario

Figure 32, Figure 33 and Figure 34 compare the cumulative cash flow evolution of the SENTINEL joint exploitation plan in the baseline scenario with each of the scenarios in the pessimistic, optimistic and uncertain cases, respectively. We observe that in all cases, even in the very pessimistic scenario, the cumulative revenues are higher than cumulative costs.

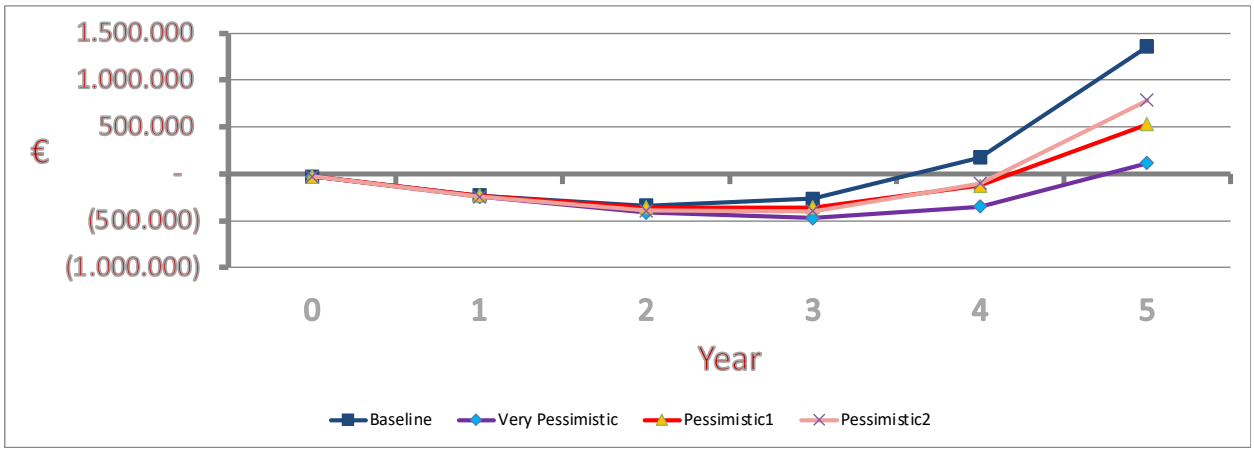

Figure 32. Comparing the cumulative cash flow evolution of Pessimistic scenarios and the Baseline scenario

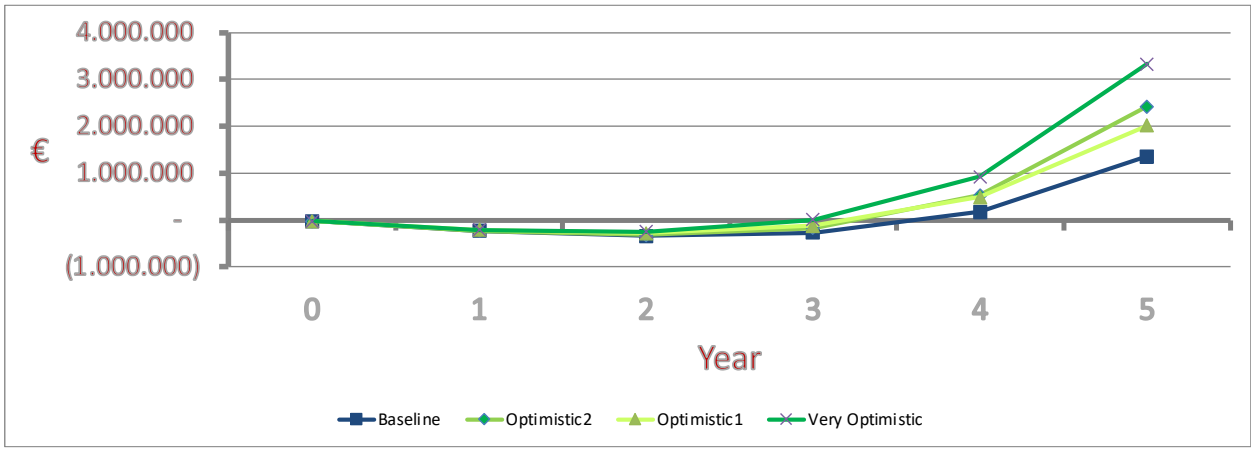

Figure 33. Comparing the cumulative cash flow evolution of Optimistic scenarios and the Baseline scenario

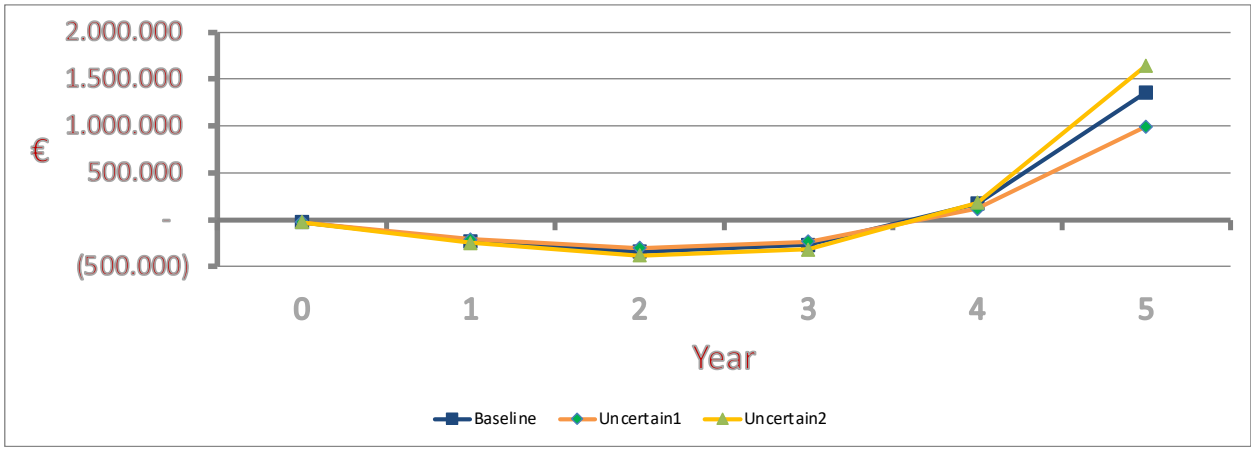

Figure 34. Comparing the cumulative cash flow evolution of Uncertain scenarios and the Baseline scenario

As expected, all pessimistic cases are less profitable compared to the baseline scenario, while optimistic ones generate operating profits that are at least 48% higher compared to baseline. Furthermore, the “Uncertain1” scenario, which involves higher number of customers at year 1 and moderate annual increase rate, is less favorable compared to the baseline one.

6.4.3 Monte Carlo simulation

In the following, we perform a Monte Carlo simulation of 100 iterations in order to consider the uncertainty related to cost estimates of the joint exploitation’s roles and the market uptake of the SENTINEL framework. In particular we assumed that each cost item and revenue stream driver is a random variable that is uniformly distributed in the range ±20% of the baseline scenario value. Then we ran 100 iterations and averaged the financial KPIs.

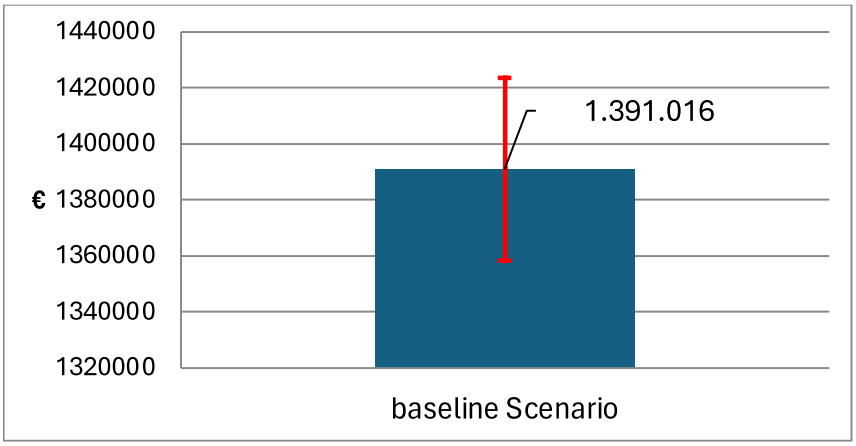

Figure 35. The average balance (and standard error in red) at year 5 for each role by performing 100 Monte Carlo simulations

Figure 35 presents the average balance at year 5 (i.e., profit) for the SENTINEL consortium. We observe that the average profit is slightly less compared to the baseline scenario. Nevertheless, uncertainty has a marginal effect on the profitability of SENTINEL joint exploitation scheme; the lower error bar suggests a sustainable outlook. Table 21 presents some interesting statistical measures, where we observe that the minimum balance witnessed in those 100 iterations was close to 700000 € (i.e., profit).

Table 21. Key statistical measures of the Monte Carlo simulation

Std. error	32.697
Min balance	693.861
Max balance	2.190.010
Std. deviation of balance	326.977

Finally, Table 22 presents the key financial metrics for SENTINEL joint exploitation based on 100 Monte Carlo iterations, where it is evident that the profitability obtained is robust to moderate uncertainty.

Table 22. Key financial metrics for SENTINEL joint exploitation scheme based on 100 Monte Carlo iterations over a 5-year period

Internal Rate of Return (IRR)	53%
Return on Investment (ROI)	75%
Present Value of FCF	952.515
Present Value of CAPEX	27.810
Present Value of OPEX	1.743.146
Present Value of Revenues	3.088.657

7. Conclusion

SENTINEL addresses a series of challenges and needs associated with data protection that affect a wide range of small businesses worldwide. These are about the GDPR and other legislation, threat of fines or reputational risk in cases of breaches, high-budget entry points to obtain enterprise-grade security and data protection, alongside an increasing complexity of IT infrastructures. SENTINEL offers them an innovative "one-stop shop" solution to (a) educate themselves and boost their overall cybersecurity and data protection awareness and preparedness; (b) become accountable by documenting (keeping records of) evidence supporting their GDPR compliance claims, including (i) using a detailed Record of Processing Activities (ROPA) to help businesses comply with Art.30 of the GDPR for keeping records of how personal data is processed and the nature and intention of data processing activities, as well as (ii) a mapping between the identified data protection requirements and the specific recommended organisational and technical measures, training material and software & tools to satisfy them; (c) reduce costs by automating assessment and policy enforcement monitoring processes and acquainting key business and technical people in the organisation with data protection compliance principles, thus saving on consultancy, training and education costs; and (d) strengthen their cybersecurity through enterprise-grade and well-integrated tools, adapted for smaller businesses.

However, competition will be tough as cybersecurity and data protection becomes increasingly attractive for both traditional players and start-ups. And while the huge interest shown by major cybersecurity players in entering the market is already a huge challenge, an even greater difficulty seems to be presented by the lack of suitable cybersecurity guidelines specific to SMEs. The ubiquitousness of digital transformation in combination with the above challenges present a dynamic market with a constantly shifting focus.

Through a series of iterations, the final business model of SENTINEL has been formulated. With the Business Model Canvas, we have visualised the SENTINEL’s unique selling proposition, value propositions, infrastructure, customers, and finances in order to align with future activities that can be adopted by the consortium towards the commercialisation of the SENTINEL offering.

This report helps the consortium understand SENTINEL’s market and prescribes a well-considered plan to tackle the various aspects of its commercialisation.

References

[1] **Mordor Intelligence (2024)**. *Europe Cyber Security Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)* [Online] Available: https://www.mordorintelligence.com/industry-reports/europe-cybersecurity-market [Accessed 31 May 2024]

[2] **MarketsandMarkets.com (2024),** *Cybersecurity Market by Offering, Solution Type, Services (Professional and Managed), Deployment Mode (On-Premises Cloud, and Hybrid), Organization Size (large enterprises and SMEs), Security Type, Vertical and Region - Global Forecast to 2028* [Online] Available: https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html [Accessed 31 May 2024]

[3] **fortunebusinessinsights.com (2024)**. *Cyber Security Market Size, Share, COVID-19 Impact & Industry Analysis, By Security Type (Network Security, Cloud Application Security, End-point Security, Secure Web Gateway, Application Security, and Others), By Enterprise Size (Small & Medium Enterprise and Large Enterprises), By Industry (BFSI, IT and Telecommunications, Retail, Healthcare, Government, Manufacturing, Travel and Transportation, Energy and Utilities, and Others), and Region Forecast, 2023-2030* [Online] Available: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 [Accessed 31 May 2024]

[4] **Mansi Shah and Paul Disselkoen (2021)**. *The Digital Opportunity: COVID-19 Pandemic Impact on European SMEs*. [Online] Available: https://publicpolicy.paypal-corp.com/sites/default/files/2021-09/EU_C19_SME_Research_Paper.pdf [Accessed 31 May 2024]

[5] **Renub Research (2023)**. *Europe Cyber Security Market, Size, Forecast 2023-2028, Industry Trends, Growth, Impact of Inflation, Opportunity Company Analysis*, [Online] Available https://www.researchandmarkets.com/report/europe-it-security-market [Accessed 31 May 2024]

[6] **statista.com (2023)**. *Technology Markets Outlook: Cybersecurity - Europe* [Online] Available: https://www.statista.com/outlook/tmo/cybersecurity/europe [Accessed 31 May 2024]

[7] **Global Industry Analysts, Inc (2024)**. *GDPR Services - Global Strategic Business Report* [Online] Available: https://www.researchandmarkets.com/reports/4805057/gdpr-services-global-strategic-business-report [Accessed 31 May 2024]

[8] **Mordor Intelligence (2024)**. *GDPR Services Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)* [Online] Available: https://www.mordorintelligence.com/industry-reports/gdpr-services-market [Accessed 31 May 2024]

[9] **databridgemarketresearch.com (2023)**. *Europe GDPR Services Market – Industry Trends and Forecast to 2030* [Online] Available: https://www.databridgemarketresearch.com/reports/europe-gdpr-services-market [Accessed 31 May 2024]

[10] **European Commission (2023)**. *Annual report on European SMEs 2022/2023* [Online] Available: https://single-market-economy.ec.europa.eu/document/download/b7d8f71f-4784-4537-8ecf-7f4b53d5fe24_en?filename=Annual%20Report%20on%20European%20SMEs%202023_FINAL.pdf [Accessed 31 May 2024]

[11] **data.europa.eu (2021)**. *Flash Eurobarometer 486: SMEs, start-ups, scale-ups and entrepreneurship* [Online] Available: https://data.europa.eu/data/datasets/s2244_486_eng?locale=en [Accessed 31 May 2024]

[12] **ENISA (2021)**. *Cybersecurity for SMEs: Challenges and Recommendation*. European Union Agency for Cybersecurity [Online] Available: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes [Accessed 31 May 2024]

[13] **ECSO (2024).** *Market Radar*. [Online] Available: https://ecs-org.eu/activities/market-radar/ [Accessed 31 May 2024]

[14] **ENISA (2016)**. *Information security and privacy standards for SMEs*. European Union Agency for Network and Information Security [Online] Available: https://www.enisa.europa.eu/publications/standardisation-for-smes [Accessed 31 May 2024]

[15] **europol.europa.eu (2021).** *Safe teleworking tips and advice - public awareness and prevention* [Online] Available: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/safe-teleworking-tips-and-advice [Accessed 31 May 2024]

[16] **ENISA (2020)**. *Tips for cybersecurity when buying and selling online* [Online] Available: https://www.enisa.europa.eu/news/enisa-news/tips-for-cybersecurity-when-buying-and-selling-online [Accessed 31 May 2024]

[17] **European Commission (2024)**. Shaping Europe's digital future – *Commission presents new initiatives for digital infrastructures of tomorrow* [Online] Available: https://digital-strategy.ec.europa.eu/en [Accessed 31 May 2024]

[18] **European Commission (2015)**. *Commission takes steps to strengthen EU cooperation in the fight against terrorism, organised crime and cybercrime* [Online] Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4865 [Accessed 31 May 2024]

[19] **European Parliament (2020)**. *MEPs demand common EU cyber defensive capabilities* [Online] Available: https://www.europarl.europa.eu/news/en/press-room/20210930IPR13930/meps-demand-common-eu-cyber-defensive-capabilities [Accessed 31 May 2024]

[20] **European Parliamentary Research Service (2021)**. *The NIS2 Directive A high common level of cybersecurity in the EU* [Online] Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf [Accessed 31 May 2024]

[21] **Wikipedia (2021).** *Business Model Canvas* [Online] Available: https://en.wikipedia.org/wiki/Business_Model_Canvas [Accessed 31 May 2024]

[22] **statista (2024).** *Number of small and medium-sized enterprises (SMEs) in the European Union from 2008 to 2023, by number of enterprises* [Online] Available: https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/ [Accessed 31 May 2024]

[23] **OECD (2022).** *The Digital Transformation of SMEs* [Online] Available: https://www.oecd.org/industry/smes/PH-SME-Digitalisation-final.pdf [Accessed 31 May 2024]

[24] **Eurostat (2023).** *Digitalisation in Europe - 2023 edition* [Online] Available: https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2023 [Accessed 31 May 2024]

[25] **European Commission (2023).** *The Digital Economy and Society Index (DESI)* [Online] Available: https://digital-strategy.ec.europa.eu/en/policies/desi [Accessed 31 May 2024]

[26] **European Commission (2023).** *Europe's Digital Decade: digital targets for 2030* [Online] Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en [Accessed 31 May 2024]

[27] **European Parliament (2022).** *Addressing the challenges of the digital transition in national RRF plans: Measures to support digitisation of SMEs* [Online] Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733734/IPOL_STU(2022)733734_EN.pdf [Accessed 31 May 2024]

[28] **Google (2022).** *Europe's SMEs in the Digital Decade 2030: Building Cyber-resilience, Overcoming Uncertainty* [Online] Available: https://storage.googleapis.com/grow-with-goog-publish-prod-media/documents/Europes_SMEs_in_the_Digital_Decade_2030_report.pdf [Accessed 31 May 2024]

[29] **Yelena Smirnova and Victoriano Travieso-Morales (2024)**, *Understanding challenges of GDPR implementation in business enterprises: a systematic literature review*, International Journal of Law and Management, 66 (3), 326-344, 2024, DOI:10.1108/IJLMA-08-2023-0170

[30] **MarketsandMarkets.com (2020),** *Security Information and Event Management Market by Component, Application, Deployment Mode, Organization Size, Vertical (Information, Finance and Insurance, Healthcare and Social Assistance, Utilities), and Region - Global Forecast to 2025* [Online] Available: https://www.marketsandmarkets.com/Market-Reports/security-information-event-management-market-183343191.html [Accessed 31 May 2024]

[31] **MarketsandMarkets.com (2018),** *Hybrid Cloud Market by Component, Service Type (Cloud Management and Orchestration, Disaster Recovery, and Hybrid Hosting), Service Model, Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2023* [Online] Available: https://www.marketsandmarkets.com/Market-Reports/hybrid-Cloud-market-1150.html [Accessed 31 May 2024]

[32] **CMS Law (2023),** *GDPR Enforcement Tracker Report* [Online] Available: https://cms.law/en/media/international/files/publications/publications/gdpr-enforcement-tracker-report-may-2023?v=1 [Accessed 31 May 2024]

[33] **statista.com (2024)**. *Share of European small businesses compliant with the General Data Protection Regulation (GDPR) in 2019* [Online] Available: https://www.statista.com/statistics/1174632/gdpr-compliance-in-small-businesses-europe/ [Accessed 31 May 2024]

[34] **statista.com (2024)**. *Share of European small businesses spending on compliance with the General Data Protection Regulation (GDPR) in 2019, by budget range* [Online] Available: https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/ [Accessed 31 May 2024]

[35] **GDPR.EU (2019)**. *GDPR Small Business Survey* [Online] Available: https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf [Accessed 31 May 2024]

[36] **European Commission (2020)**. *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation* [Online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264 [Accessed 31 May 2024]

[37] **Palqee Technologies (2021)**. *SME's struggle the most with data privacy regulations* [Online] Available: https://medium.com/palqee/smes-struggle-the-most-with-data-privacy-regulations-3fde68a98281 [Accessed 31 May 2024]

[38] **Thomson Reuters (2019)**. *Top five concerns with GDPR compliance* [Online] Available: https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance [Accessed 31 May 2024]

[39] **Ecomply (2020)**. *GDPR Readiness Survey for Software and SMEs* [Online] Available: https://www.ecomply.io/blog-en/gdpr-readiness-survey-software-and-smes [Accessed 31 May 2024]

[40] **Cyberwatching (2024)**. *Cybersecurity and Privacy research results for a resilient Europe* [Online] Available: https://cyberwatching.eu/ [Accessed 31 May 2024]

[41] **European Cybersecurity Month (2024)**. *European Cybersecurity Month Campaign* [Online] Available: https://cybersecuritymonth.eu/ [Accessed 31 May 2024]

[42] **Junglemap (2024)**. *GDPR & Privacy Awareness* [Online] Available: https://www.junglemap.com/GDPR-courses [Accessed 31 May 2024]

[43] **Windley, Phillip J. (2022)**, *Delivering High Availability Services Using a Multi-Tiered Support Model*, Windley's Technometria [Online] Available: https://www.windley.com/docs/Tiered%20Support.pdf [Accessed 31 May 2024]