SENTINEL - Approachable, tailor-made cybersecurity and data protection for small enterprises

Tatiana Trantidou
Information Technology for Market Leadership (ITML) IKE
Athens, Greece
0000-0001-6784-2665

George Bravos
Information Technology for Market Leadership (ITML) IKE
Athens, Greece
0000-0002-6180-0138

Philippe Valoggia
Luxembourg Institute of Science and Technology
Esch/Alzette, Luxembourg
0000-0002-4294-0848

Ioannis Skourtis
Institute of Digital Innovation and Research (IDIR) Limited
Dublin, Ireland
yannis@idir.eu

Manolis Falelakis
Intrasoft International
Luxemburg
0000-0002-3620-4668

Kostas Poulios
Sphynx Technology Solutions AG
Switzerland
k.poulios@sphynx.ch

Ilias Spais
R&D
AEGIS IT Research
Braunschweig Germany
hspais@aegisresearch.eu

Sotiris Ioannidis
School of Electrical and Computer Engineering
Technical University of Crete
Chania, Greece
0000-0001-9340-2241

Thomas Oudin
AIRBUS CyberSecurity
Elancourt France
Thomas.oudin@airbus.com

Ruben Costa
CTS-UNINOVA and School of Science and Technology, NOVA University of Lisbon
Caparica, Portugal
0000-0002-6142-1840

Christopher Konialis
ClinGenics
London, United Kingdom
c.konialis@clingenics.co.uk

Daryl Holkham
Tristone Capital Ltd
Manchester, United Kingdom
line 5: email address or ORCID

Zoe Kasapi
Centre for European Constitutional Law
Athens, Greece
projects@cecl.gr

Athanasios Karantjias
Focal Point sprl
Braine l'alleud, Belgium
0000-0002-3365-0785

***Abstract* — Over 25 million Small and Medium Enterprises (SMEs) in Europe face multiple challenges related to personal data protection (PDP), ranging from awareness of EU's General Data Protection Regulation (GDPR) to a clear and practical roadmap to compliance. Many also cannot afford access to enterprise-grade cybersecurity technology. This paper presents the main objectives and innovations of the EU-funded SENTINEL project, which introduces the concept of *Intelligence for Compliance*; it integrates tried-and-tested modular cybersecurity and privacy technologies with fresh, ambitious ones, such as a novel Identity Management System (IdMS) for human-centric data portability, and an end-to-end PDP compliance self-assessment framework. Combined with machine learning powered recommendations, policy drafting and enforcement for compliance, and a set of plugins that contains cybersecurity, data privacy and simulations/training software tools, SENTINEL aims to help small enterprises feel considerably more secure by safeguarding their and their customers' assets.**

Keywords—cybersecurity, privacy and data protection, cyber-threat intelligence, AI, identity management, self-compliance

I. INTRODUCTION

The European Union's currently over 25 million Small and Medium-sized Enterprises (SMEs), lying centre-stage within EU enterprise policy, are facing multiple challenges related to data protection and General Data Protection Regulation (GDPR) compliance. These challenges range from awareness, access to affordable professional legal advice/consulting and related capacity-building, to a clear, actionable, and practical roadmap to compliance. Combined with the perceived complexity introduced by data privacy, security, portability and governance requirements, the need for robust Small and Medium-sized Enterprises and Micro Enterprises (SME)-specific support measures is obvious and warranted, as also dictated by GDPR's r.132 [1]. Fines from supervisory authorities in the EU can reach up to 20 million Euros or 4% of annual global revenues, whichever is greater. Protecting the rights of data subjects is a serious business, and as the value of personal data rises, so could fines [2].

Around half of small businesses are failing GDPR compliance on two crucial requirements: (i) The GDPR requires companies to describe data processing activities in clear, plain language to data subjects; and (ii) it requires businesses to identify a lawful basis for using someone's data. According to a very recent study [3], managers of small and micro businesses are often confused about basic data security concepts, like data stewardship, encryption and secure communication. Nevertheless, they appear open to invest in regulatory compliance since over half of small businesses report spending between €1,000 and €50,000 on

GDPR compliance, including expenses for consultants and technology. However, according to the same study, millions of European SMEs still do not fully comply with the GDPR. This presents an imbalance between security- and privacy-related spending and its actual effect on personal data protection (PDP) and compliance for SMEs.

We perceive this imbalance as an opportunity and key driver behind the vision of the SENTINEL project. In this respect, the SENTINEL project [4] proposes a novel "one-stop shop" approach to integrated and obtainable privacy and personal data protection compliance for SMEs, based on a rationale described in the following analysis. SENTINEL aspires to bridge the security and personal data protection gap for European SMEs by raising awareness and boosting their capabilities in the domain through innovation at a cost-effective level. This vision will be realized by integrating tried-and-tested security and privacy technologies into a unified digital architecture and then applying disruptive *Intelligence for Compliance*. Combined with a well-researched methodology for application and knowledge sharing and a wide-reaching plan for experimentation for innovation within SMEs, SENTINEL aims to help small enterprises feel considerably more secure and safeguard their and their customers' assets.

This paper is organized as follows: Section II, provides an analysis of the related work and points out, how SENTINEL goes beyond the state-of-the-art; Section III, describes the SENTINEL concept and its components; In section IV, an analysis of the validation use-cases is provided; finally, section V concludes the paper and references future work.

II. Related Work

With respect to the related work, SENTINEL innovates in 4 domains: (i) Identity Management for Data Portability; (ii) GDPR compliance; (iii) Cyber Ranges; and (iv) Requirements Engineering (RE), applied to the privacy and personal data protection challenges of SMEs.

A. *Identity Management for Data Portability*

The right to data portability presupposes acting drastically at the architecture level of data flow. According to the GDPR, the mere exchange of CSV spreadsheets allows to operationalise data portability. Even if such approach were lawful, it would not be an efficient way to foster the free flow of personal data. Direct transmission from the personal data holder (i.e., controller) to another one is a more promising way. Until recently there were two models used to support personal data interchange: the API model and the Aggregator model. However, five years ago, MyData (also commonly referred to as the Nordic model) [5] introduced a new paradigm in personal data management and processing by adopting a human-centric perspective. This ambitious model aimed at giving individuals total control over their personal data, transforming them from passive targets to empowered actors in the management of their personal lives. Although SMEs will not be holders of personal data, they will serve as activists/evangelists of the emerging architecture, a role which large organizations and current data aggregators are often unable or unwilling to fulfil. SENTINEL's IdMS (Identity Management System for Data Portability) component delivers this vision to SMEs as a service. From a GDPR compliance perspective, the IdMS implementation allows participants to fully access or modify their data and easily audit who accessed it (in full compliance with GDPR). End users are able to grant or deny access to any organization they choose. Since trust is the most important component of success, with IdMS, data are securely stored with the centralized IdMS infrastructure in the way described by the model (MyData operator). In this way, personal data can be effectively held by the end users themselves, allowing them to be the 'physical' owners. A standard protocol is defined as a proof-of-concept to allow the IdMS to be totally independent of the platforms used by SMEs or individuals, removing the need for third parties and integrations.

B. *GDPR compliance*

One key aspect of GDPR is its compliance regime. While regulations are usually prescriptive in telling regulated entities what to do and how to do it, GDPR only establishes data protection principles that must be respected. Because this regulation does not specify how to meet expected requirements, it is up to regulated entities to select and "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with [GDPR]" (GDPR, Art. 24.1). Regulated entities become "responsible for, and be able to demonstrate" compliance when handling personal data; they have to be "accountable" (GDPR, Art. 5.2) [6] regarding the protection of personal data. Compliance determination requires then more than a tick boxing approach; it requires an inspection of Organizational and Technical Measures (OTMs) implemented to meet GDPR requirements. Determining whether OMTs implemented are appropriates and effectives measures to preserve privacy and data protection increases compliance efforts regulated entities must make. GDPR compliance burden is likely to become a huge hurdle to SMEs. Digitalization of an existing GDPR compliance assessment method [Ref] can help them to jump it more easily.

As other compliance inspection approaches as audit, GDPR Compliance Assessment requires the involvement of experts that can combine several fields of knowledge. Compliance with GDPR implies to combine at least legal and technical expertise. to both identify and determine whether OTMs are appropriates and effectives. Digitalization of this method supposes to transfer part of expert's knowledge to a rules engine system. Expert's knowledge to capture and formalize is about 1) OTMs that can be implemented to meet GDPR requirements, and 2) rules to determine compliance assessment results. Such knowledge frames engine rules allowing SMEs to self-assess and demonstrate compliance with GDPR.

C. *Cyber ranges*

In general, cyber ranges are often specified as technical environments that simulate ICT infrastructures [7]. Cyber ranges have become a service to support hands-on training and cyber defence exercises to increase the resilience of organisations when facing cyber incidents or cyber-attacks. The current state-of-the-art for cyber range leverages the underlying capabilities of Infrastructure as a Service (IaaS) technologies as a host environment and Platform as a Service (PaaS) cloud technologies for orchestration, creating a virtualisation environment in which virtual machines representing a simulation scenario can be hosted on an available hardware.

In SENTINEL the real-time cyber range training services focus on the easier and usable training service provision for SMEs and, therefore, the following challenges are addressed beyond the state-of-the-art: (i) A decision support algorithm and implementation for the cybersecurity training self-assessment of SMEs provides a graphical user interface for the interactive and dynamic self-assessment of the SMEs. During the assessment, SMEs define their current status of cyber situational awareness and receive a customized training plan matching to their capability needs and challenges; (ii) A usable graphical interface for the SME real-time cyber range training service allows the utilization of the self-assessment results and the display of suggested trainings, but also the management of evaluation reports of conducted trainings. Standardized formats support the training service capabilities and can be compared to other trainings (e.g., goals, tasks, achievements, etc.); (iii) An evaluation software component allows monitoring of the cyber training scenario events and event triggers at run-time, under operator control, as well as assessment of the quality of actions of the trainees during the simulation.

D. *Requirements Engineering (RE), applied to the privacy and personal data protection challenges of SMEs*

Cybersecurity requirements aim to deflect unauthorised manipulation of information systems - be it interferences with the system environment or intentional manipulations of unauthorised entities [8]. Enterprises, regardless of their size, must manage the cybersecurity risks to improve the security and resilience of their assets. In the case of SMEs, additional challenges present themselves because of the lack of resources and relevant in-house expertise [9]. Traditional Security Requirements Engineering (SRE) methodologies fall mainly in two categories: risk-oriented and goal-oriented.

In risk-oriented SRE approaches, cybersecurity is defined as the protection of assets through the treatment of threats that put information at risk. Prominent amongst these approaches are those that are propagated by standardization organizations such as ISO, ENISA, NIST. Risk-oriented approaches exploit existing knowledge sources, which fall into three types [10]: (a) knowledge about possible threats and associated assets (threat taxonomies and asset taxonomies), regarded as *diagnostic knowledge*; (b) knowledge about relevant security guidelines and security (design) patterns, regarded as *prescriptive knowledge*; (c) knowledge about legally binding or contractually agreed requirements, i.e., *compliance obligations*.

Goal-oriented SRE approaches attempt to firstly define the system's social environment and boundary, identify the potential stakeholders of the systems and analyze their intentions in order to elicit and specify business requirements [11]. The emphasis of goal-oriented SRE is on late requirements. This means that goal oriented SRE approaches treat security requirements as the operationalization of stakeholder goals and neglect strategic issues.

With the advent of cloud computing a recent trend is the consideration of security provision as a service [12], [13]. In this context, SRE does not focus on in-house security mechanism specification, rather it concerns the identification of the appropriate security services offered by external providers that meet the business security requirements. This service-oriented trend raises the need for a new SRE metaphor that will enable the mapping of business security requirements onto external or internal service provision through appropriate capabilities. A taxonomy of capabilities into nine different domains has been reported [14].

In the SENTINEL project, we deploy an extension of the eCORE method [15], that has been applied on a variety of domains [16], [17], referred to as the SCORE (Security Capabilities Oriented Requirements Engineering). The positioning of SCORE in SENTINEL is based on two objectives. First, it is used to identify the challenges and needs for data privacy and compliance processes in SMEs, thus ensuring that the SENTINEL framework meets these challenges and needs in a most effective and efficient manner. Second, it is used as a generic RE methodology, specifically targeting SMEs to address their specific needs and capabilities in such a way, so as to enable these companies to yield the benefits of using the SENTINEL framework.

III. SENTINEL CONCEPT

The SENTINEL project delivers a solution that enables a novel "one-stop shop" approach to integrated and obtainable private and personal data protection compliance for SMEs. This will be achieved through the adherence to the following propositions (Figure 1):

- Delivering a robust, technologically feasible and usable digital architecture that will provide SMEs security and privacy functionalities hitherto unavailable outside the domain of large enterprises.
- Offering the SENTINEL users a theoretically relevant detailed methodology for the effective utilisation of this digital framework.

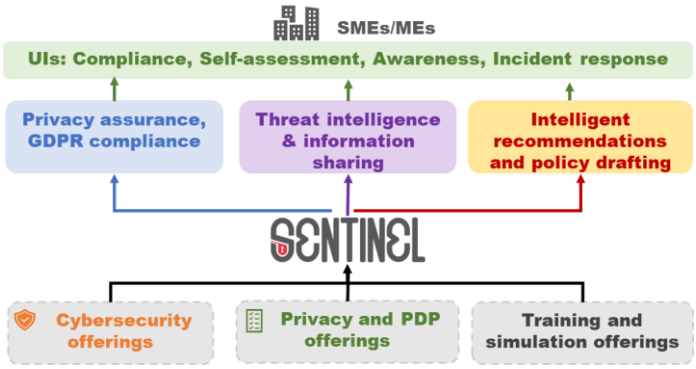

Fig. 1. The SENTINEL high-level concept and set of services

- Allowing for extensive experimentation on three carefully chosen pilots from three different business domains, featuring sensitive personal data protection requirements.
- Reaching out to over 10.000 smaller enterprises across at least six (6) countries to roll out this novel approach.

The remainder of this section is dedicated to elaborating on these principles, thus demonstrating the novelty, the relevance, the feasibility and the value of SENTINEL in the way that SMEs will benefit from well-designed, intelligent, and decentralised privacy and personal data protection management services without the need for dedicated human resources or know-hows.

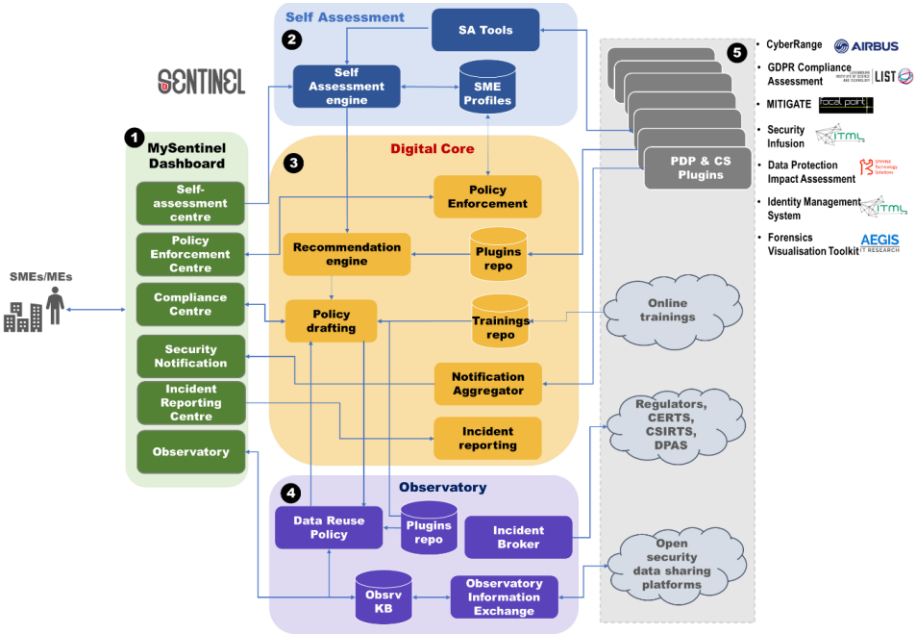

Fig. 2. SENTINEL framework architecture

A systemic view of the architecture is shown in Figure 2. The description herein focuses on the logical structure of the architecture providing (a) an overall view for it, (b) the rationale for each component in its relation to other components, (c) the building blocks for delivering the components that include existing technologies contributed by the SENTINEL participants as well as new solutions developed within the project and (d) the way that the users may deploy this architecture in such a way, so as to empower SMEs to tackle their specific needs and accordingly to establish appropriate internal security and privacy capabilities.

To facilitate readability of the conceptual architecture diagram in Figure 2, the components of SENTINEL are numbered (1 to 6) and are presented in this order. The numbering follows the user flow.

(1) The MySentinel Dashboard offers a set of front-end modules to facilitate corresponding interactions between the user and the SENTINEL's services. The set comprises the following front-end modules: (a) self-assessment centre; (b) policy enforcement Centre; (c) Compliance Centre; (d) Security Notifications; (e) Incident Reporting Centre; (f) Observatory.

(2) The Self-assessment context provides modules that manage SMEs' profiles, requirements, trainings and assessment by means of RASE (Risk Assessment for Small Enterprises) score – a multifactorial storage object which is created following the participant's initial profiling (requirements elicitation). The containing modules are: (a) the Self-Assessment (SA) Engine, which processes an SME requirements and profile to produce lists of recommended trainings and RASE scores; (b) SA tools, an interface to the available self-assessment plugins; (c) SME profiles repository, where profiles, RASE scores and progress for each participating SME is stored.

(3) The Digital Core groups all main intelligent modules that aim to address an SME's security concerns in various ways. This component includes the following modules: (a) the recommendation engine, which provides an optimal combination of available plugins to address vulnerabilities and shortcomings of an SME's infrastructure and internal processes, based on the calculated RASE score; (b) the policy drafting module, which processes the recommendation engine's output in order to produce a policy draft with structured, actionable policy elements; (c) the policy enforcement module, which helps users follow the process of executing or applying a policy recommendation; (d) the notification aggregator module, which notifies the end-users about security incidents identified by any of the recommended plugins; (e) the incident reporting module, which helps end-users submit observed incidents and share them to external sources, in anonymised manner; (f) the Plugins repository, a store that contains all available plugins, their capabilities and configuration options; (g) the Trainings repository, a store that contains all available training tools offered to participating SMEs.

(4) The Observatory constitutes the interface of SENTINEL to the outside world by sharing and receiving anonymised security-related findings. It offers the following modules: (a) the Observatory Knowledge Base (KB), a store with a wide spectrum of security-related information, collected from external sources and updated with anonymised findings from SMEs registered with the SENTINEL platform; (b) the data reuse policy module, which identifies and shares patterns of reusable policy elements, assisting the creation of policy drafts, as well as updating the Observatory KB with useful policy information; (c) the Incident broker module, which interfaces end-user submitted incidents to external sources; (d) the Observatory Information Exchange, an API (Application Programming Interface) that periodically polls external sources for newly identified security-related information, and also shares findings stored in the Observatory KB with the outside world; (e) the. Policies repository, a store that collects atomic, independent, validated policy elements that can be used for policy drafting and policy reuse.

(5) External entities, plugins, and sources that are external to SENTINEL, including a list of available plugins, online trainings, open security data sharing platforms, and regulating entities such as CERTs (Computer Emergency Response Teams), CSIRTs (Computer Security Incident Response Teams) and DPAs (Data Protection Authorities). The compilation of plugins comprise both proprietary

software tools that are customised and further improved within SENTINEL (e.g., Security Infusion [18], MITIGATE [19], [20], CyberRange [21], Data Protection Impact Assessment [22], Forensics Visualisation Toolkit [23], GDPR Compliance assessment tool [24]), as well as newly developed modules within the project, such as the Identity Management System, and open-source modules that all enrich the variety of offerings in SENTINEL. This pluggable approach to the architecture allows any tool or technology that offers valuable cybersecurity and/or data privacy capabilities to be plugged on the core SENTINEL architecture.

IV. USE-CASES AND VALIDATION

SENTINEL's offerings will be validated via seven indicative use cases in real-world SME settings:

1. *SME registration and profiling*: The SME representative registers the company and fills in the related questionnaire. Based on this information, the system produces a profile of the company.
2. Completing a self-assessment workflow: The user completes a self-assessment workflow that has been proposed by the SENTINEL platform, after gathering the SME requirements during registration.
3. Acquiring policy recommendations: The SME representative fills out the company security profile and performs related self-assessment tasks indicated by the system. Then they receive a tailor-made set of security policies.
4. Receiving security notifications: The system detects a CS or PDP incident that affects an SME and alerts the SME representative to attend to it.
5. Policy enforcement monitoring: The SME representative provides an update to the system concerning the status of implementation of policies they have received as recommendations from the SENTINEL platform.
6. Consulting the Observatory Knowledge Base: The SME browses the SENTINEL Observatory Knowledge Base and accesses information about recently identified data and privacy breaches. The Knowledge Base is continuously updated and synchronized with external resources.
7. Incident reporting and sharing: A security incident has been detected and the SME wants to report and share it with appropriate response teams and/or open security data platforms, such as malware information sharing and incident response hubs.

Based on the above use cases, the SENTINEL framework validation in real-world settings is facilitated by two distinct enterprises in the fields of genomics and social care.

A. *Microenterprise test case*

The focus of this test case is to implement extra security measures for accessing genomic sequence and personal data from a bioinformatics platform software pipeline.

The company's work is based on EMA - Exome Management Application: a bioinformatics platform-software pipeline, coupled to expert curation for the evaluation and reporting of actionable genomic variants. The EMA pipeline software provides sic (6) types of variant data interpretation services, plus a dedicated custom variant analysis upon request. The company handles human DNA sequence variants, human phenotype and disease related info, anonymized demographic data and technical experimental data. The company maintains an internal database containing user/customer-related information submitted during registration.

The types of anonymous data submitted by the users and maintained by the company include: (1) Human DNA sequence variants, generated typically by Next Generation Sequencing (NGS) applications and submitted by the users for variant prioritization and interpretation, (2) standardized, in Human Phenotype Ontology - HPO format, phenotype and disease related information related to and accompanying the specific co-submitted (1) data file (see above), (3) simple anonymous proband demographic data, such as gender, age, ethnicity, disease status (affected or not) and relevant disease inheritance information, (4) technical/experimental data, relating to the type of NGS analysis, platform utilized, etc.

Although all proband/patient related data submitted by the users are totally anonymous, without any type of personal identifiers, bearing in mind that genomic sequence data constitute per se sensitive and precious personal data, the company wishes to have further layers of security regarding the access of data stored in the proband database module of the EMA pipeline. Not relying solely on anonymization, SENTINEL envisages implementing extra security measures, for example i) a more secure user login process, scanning for the presence of any personally identifiable information (PII) during the submission process, ii) specific cyber security protection of all stored data, and iii) to generally put in place appropriated systems that limit any type of unauthorized access to the data.

B. *Small-Medium Enterprise*

The focus of this test case is to homogenise the approach to data protection and compliance across multiple portfolio business through a single platform.

The SME is an investment company committed to the acquisition and growth of established, profitable and cash generative companies that deliver positive social impact. The company invests in projects that fall into one of the following categories: (a) Registered children's homes; (b) Specialist care facilities; (c) Specialist education facilities; (d) Fostering services; (e) Specialist adult care facilities; and (f) Social care training companies.

The company and its portfolio businesses collect and use personal information from users of their services. This information is gathered as is consistent with the company's duty as a responsible provider of regulated and unregulated social care. In addition, the company may be required by law to collect, use and share certain information. The security and privacy of data both within the organisation and as transmitted between social care agencies (i.e., Local Authorities, the Police etc.) is of paramount importance. The different types of data processed by the company, can be described as follows: (i) Financial and Operational Data – financial and operational data of portfolio companies as well as that of potential acquisition targets; (ii) Social Care Data – information concerning service users is referred into each social care organisation, which then builds up a profile of service user data as the service user is supported by the company; and (iii) Staff Data – following stringent safer recruitment processes to protect the wellbeing of the company's service users is critical. The company, therefore, gathers a substantial amount of personal and sensitive data when recruiting, which is regularly updated.

Security and privacy are currently being handled within the company's portfolio businesses using multiple platforms with little consistency either within one business on its own or across all the company's businesses. With increasing reliance on networking and remote working, the security and privacy of the company's data is more pressing than ever before. The ambition of the company is to homogenise their approach to cybersecurity across the entire portfolio of businesses and to provide a single platform to handle all requirements in a most effective and efficient way.

V. CONCLUSIONS & FUTURE WORK

The main objective of this paper was to present the main objectives and innovations of the H2020 SENTINEL project. SENTINEL proposes a novel "one-stop-shop" approach to integrated and obtainable privacy and personal data protection compliance to SMEs. Its main capabilities focus on: (i) assessing of the current privacy and data protection risks of SMEs; (ii) drafting and enforcing a unified GDPR-compliant privacy and data protection policy addressing the identified gaps; and (iii) collecting, analysing and sharing critical privacy incident or data breach information using proprietary and open-access platforms to facilitate both reporting to DPAs and responding faster to privacy-related threats. Future steps involve further development of the SENTINEL's modules and contexts, as well as validation of various use cases in real-world enterprise settings.

ACKNOWLEDGEMENTS

The authors acknowledge the European Commission for the support and funding under the scope of Horizon2020 SENTINEL Project (Grant Agreement Number 101021659) and the partners of the SENTINEL Project Consortium.

REFERENCES

[1] European Comission, "Recital 132 EU GDPR," 28 February 2022. [Online]. Available: https://www.privacy-regulation.eu/en/recital-132-GDPR.htm.

[2] SecurityMetrics, "How Much does GDPR Compliance Cost?," [Online]. Available: https://www.securitymetrics.com/blog/how-much-does-gdpr-compliance-cost. [Accessed 28 February 2022].

[3] GDPR.EU, "GDPR Small Business Survey - Insights from European small business leaders one year into the General Data Protection Regulation," 2019.

[4] SENTINEL Consortium, "SENTINEL," 01 June 2021. [Online]. Available: https://sentinel-project.eu/. [Accessed 25 February 2022].

[5] K. Kuikkaniemi, A. Poikola and H. Honko, "MyData A Nordic Model for human-centered personal data management and processing," white paper, 2015.

[6] intersoft consulting, "Art. 5 GDPR - Principles relating to processing of personal data," intersoft consulting, [Online]. Available: https://gdpr-info.eu/art-5-gdpr/. [Accessed 2 MArch 2022].

[7] National Institute of Standards and Technology, US, "Cyber Ranges," U.S. Department of Commerce National Institute of Standards and Technology, [Online]. Available: https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf. [Accessed 25 February 2022].

[8] C. Ebert, "Cyber Security Requirements Engineering," in *Requirements Engineering for Service and Cloud Computing*, Springer, 2017, pp. 209-228.

[9] M. Benz and D. Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," *Business Horizons*, vol. 63, no. 4, pp. 531-540, 2020.

[10] C. Schmitt and P. Liggesmeyer, "Instantiating a model for structuring and reusing security requirements sources," in *IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)*, Ottawa, Canada, 2015.

[11] P. Meland, E. Paja, E. Gjære, S. Paul, F. Dalpiaz and P. Giorgini, "Threat Analysis in Goal-Oriented Security," *Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications*, pp. 2025-2042, 2018.

[12] D. J. Feher and B. Sandor, "Cloud SaaS Security Issues and Challenges," in *13th International Symposium on Applied Computational Intelligence and Informatics*, 2019.

[13] U. Noor, Z. Anwar, J. Altmann and Z. Rashid, "Customer-oriented ranking of cyber threat intelligence service providers," *Electronic Commerce Research and Applications*, vol. 41, 2020.

[14] F. Ghaffari and A. Arabsorkhi, "A New Adaptive Cyber-security Capability Maturity Model," in *9th International Symposium on Telecommunications*, Tehran, Iran, 2019.

[15] P. Loucopoulos, E. Kavakli, D. Anagnostopoulos and G. Dimitrakopoulos, "Capability-oriented Analysis and Design for Collaborative Systems: An example from the Doha 2022 World Cup Games," in *10th International Conference on Computer and Automation Engineering*, Brisbane, Australia, 2018.

[16] G. L. P. D. G. A. D. &. K. V. A. Bravos, "Capability – Driven modelling approach applied in smart transportation & management systems for large scale events," *EAI Endorsed Transactions on Internet of Things*, vol. 3, no. 9, pp. 1-8, 2017.

[17] G. Dimitrakopoulos, E. Kavakli, P. Loucopoulos, D. Anagnostopoulos and T. Zographos, "A capability-oriented modelling and simulation approach for autonomous vehicle management," *Simulation Modelling Practice and Theory*, vol. 91, pp. 28-47, 2019.

[18] ITML, "ITML Infusion Datasheet," 2020. [Online]. Available: https://www.itml.gr/sites/default/files/docs/ITML_Infusion_Datasheet_1020.pdf. [Accessed 10 March 2022].

[19] S. &. P. D. Papastergiou, "Securing maritime logistics and supply chain: The medusa and mitigate approaches.," *Maritime Interdiction Operations*, vol. 14, no. 1, pp. 42-48, 2017.

[20] S. P. N. &. M. H. Schauer, "MITIGATE: A dynamic supply chain cyber risk assessment methodology.," *Journal of Transportation Security*, vol. 12, pp. 1-35, 2019.

[21] AIRBUS, "CyberRange Cyber Attack Simulation Services," AIRBUS, 2022. [Online]. Available: https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/. [Accessed 11 March 2022].

[22] Sphynx Technology Solutions AG, "Products," Sphynx Technology Solutions AG, 2022. [Online]. Available: https://www.sphynx.ch/products/#assurance-platform. [Accessed 10 March 2022].

[23] AEGIS, "Forensics Visualization Toolkit (FVT)," [Online]. Available: https://aegisresearch.eu/solutions/forensics-visualization-toolkit-fvt/. [Accessed 7 March 2022].

[24] S. Cortina, M. Picard, S. Renault and P. Valoggia, "Towards a Process-Based Approach to Compliance with GDPR," in *Systems, Software and Services Process Improvement. EuroSPI 2021. Communications in Computer and Information Science*, Krems, Austria, 2021.