Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Apply the principles and practices of Data security, Governance and Compliance based on a FinSure Bank.

Student Name: Khadija Banu

Student ID: 2527944

Programme: MSc Cybersecurity and Digital Forensics

Module: Data Security, Governance and Compliance (ACCA7028)

Lecturer: Dr. Ayman Al Hajjar

Submission Deadline: 29th April 2026 (2PM)

Table of Contents

1. Abstract
2. Introduction
3. Assumptions
4. Evaluation of Security Frameworks and Models
    4.1 ISO/IEC 27000 Series (ISMS)
    4.2 Information Technology Infrastructure Library (ITIL)
5. Designed Approach for Finsure Bank
    5.1 Governance and Strategic Planning
    5.2 Security Policies & BYOD Risk Management
    5.3 Active Defense & SIEM Implementation
    5.4 Compliance (GDPR) & Protection Mechanisms
    5.5 Contingency Planning and SLAs
6. Critique of Dynamic Regulations and Standards
    6.1. The Asymmetric and Evolving Threat Landscape
    6.2 Fast Technological Innovations and Architectural Changes
    6.3 Ethical Responsibility and the Consumer's Right to Privacy
7. Conclusion
8. References

1. Abstract

FinSure Bank, being a highly dynamic financial services firm with operations in numerous countries, is driven by its online banking, savings, loan, and investment services. As a result, its IT infrastructure is highly cloud-based, with more than 90% of its infrastructure being externally located. However, with an increase in Bring Your Own Device (BYOD) culture in its business operations, It is also exposed to numerous cybersecurity threats. Currently, despite dealing with highly sensitive financial data, The bank lacks an effective governance model, security policy, or regulatory compliance. This report outlines a strategic intervention plan using the ISO 27000 security framework [1]. Moreover, it also proposes an active defense architecture using a Security Information and Event Management (SIEM) strategy [2]. Using customized log analysis for distributed cloud environments, it aims at mitigating insider threats, ensuring high levels of GDPR compliance, and protecting its sensitive assets.

2. Introduction

With the rise in the demand for online financial services worldwide, institutions face the challenge of ensuring data security while providing easy access to their services. The rise of internet-based platforms has led to an expectation of easy access to information and services, but it also presents an expanded threat of cyber attacks and other related risks. With billions of people worldwide having access to information online, the threat of cyber attacks by individuals, organizations, and government agencies is increasing every day.

FinSure Bank, which is expanding rapidly and offering diverse financial services online, is highly dependent on infrastructure that is over 90% hosted in the cloud and is facing the challenge of implementing BYO16D practices in the workforce of diverse employees, contractors, and partners, who are also expanding in line with the operations of the bank. The rise in

the use of mobile banking applications by the bank's clients has also led to critical risks of data privacy, identity theft, online fraud, and severe cyber attacks.

Currently, the information security posture of the institution is highly fragmented in nature. The organization is running without a unified governance structure, risk management strategy, and compliance audits. The lack of comprehensive information security policies makes the organization highly vulnerable to cyber attacks and other security breaches. Moreover, there are rising concerns from within the organization regarding the security of sensitive financial data, intellectual properties, and adhering to data protection laws such as the GDPR [3].

To address the aforementioned critical information security vulnerabilities, this report undertakes an in-depth analysis of the information security frameworks that are already in place in the market, with a major emphasis on the ISO 27000 series and ITIL frameworks. Based on the information security principles of these frameworks, this report proposes an information security, governance, and compliance architecture suitable to the organizational requirements of the bank. The organization can easily overcome the risks associated with its cloud infrastructure and BYOD strategy by adopting a unified information security and governance strategy based on SIEM log analysis.

3. Assumptions

While developing an effective security posture and governance approach for FinSure Bank, there are certain basic assumptions that need to be defined in relation to the operational state of the bank and its technology stack.

- Cloud Architecture and Responsibility: It is assumed that the financial provider is using a major Tier-1 cloud infrastructure provider (for example, Amazon Web Services or Microsoft Azure) for hosting its

90% external infrastructure. Therefore, it is assumed that the bank is using a Shared Responsibility Model [4], in which the infrastructure provider is responsible for securing the physical infrastructure, but it is entirely responsible for securing customer data, identity access management, etc.

- Containerized Microservices: Due to the digital native and growth-oriented nature of the organization, it is assumed that the institution utilizes microservices containers, such as Docker containers, and runs them using Kubernetes to deploy and scale their digital banking applications in a Linux environment.

- BYOD Access Mechanisms: It is assumed that employees, contractors, and other business partners who wish to access the organization's resources through their own devices (BYOD) are required to access the organization's resources securely through a client-based Virtual Private Network (VPN) solution with Multi-Factor Authentication (MFA).

- Executive Buy-In and Budget: Although the bank has not yet developed a unified governance strategy, it is assumed that the executive management is fully committed to ensuring compliance with regulations and has allocated an adequate budget to address the security remediation activities, in particular, the acquisition of a Security Information and Event Management (SIEM) solution.

4. Evaluation of Security Frameworks and Models

From an unstructured and ad-hoc approach to securing one's infrastructure to a more mature and GDPR-aligned architecture necessitates the use of standards from the industry. Yet, frameworks cannot be treated as silver bullets that automatically resolve the problem at hand and need to be carefully scrutinized in their context of application. In this section, the

appropriateness, practical difficulty, and value of two key frameworks – ISO/IEC 27000 suite and ITIL – will be discussed.

4.1. ISO/IEC 27000 Series (ISMS)

The International Organization for Standardization (ISO) 27000 family is a globally recognized set of standards that provides a systematic and risk-based approach to the management of sensitive information held by companies [1]. The most important standard in this family is the ISO/IEC 27001 standard, which requires the establishment, implementation, maintenance, and continual improvement of an Information Security Management System (ISMS).

For the institution, which deals with highly sensitive financial information and has no formal controls in place for regulatory compliance, the implementation of an ISMS is a strategic necessity. ISO 27001 will require the organization to shift its mindset to a more proactive approach to security rather than the reactive approach that is common in the industry. The standard requires the organization to constantly perform risk assessments. This addresses the risks that it faces in the areas of online fraud, identity theft, and the increasing risks that BYOD poses to the organization [1].

4.2. Information Technology Infrastructure Library (ITIL)

Although the ISO 27000 series represents the authoritative design blueprint for security governance, ITIL 4 represents an all-encompassing framework for IT Service Management (ITSM) in general, ensuring that IT services are perfectly aligned with overarching business goals and objectives [5]. ITIL focuses on agility, automation, and the seamless integration of security into the entire service value chain.

For the digital-first provider that operates virtually all aspects of the business via cloud-based technologies, ITIL is critical in the management

of the digital banking services lifecycle. The Information Security Management practice under the ITIL framework ensures that active defense technologies are incorporated into new services rather than merely adding them after the fact [5]. For instance, in the process of rolling out the BYOD strategy at the bank to incorporate third-party partners and contractors, ITIL dictates the formal process of incident management, change control, and service level management.

5. Designed Approach for FinSure Bank

In order to ensure that the severe operational and regulatory weaknesses arising from the aggressive growth and utilization of cloud-native computing of the enterprise will be addressed, a cohesive and integrated security architecture should be considered. As shown in Figure 1 below, the FinSure Bank Security Framework seeks to integrate what has been previously used in the bank as a disjointed system in order to provide a cyclical defense strategy. The framework is designed based on the core principles of the ISO/IEC 27000 series and ITIL, divided into five pillars.

This process starts with Governance & Strategic Planning in order to ensure alignment between the goals of the organization and the security measures adopted. Security policies and BYOD management will be developed in order to provide a comprehensive defense framework in line with the principles of Zero Trust Architecture for securing unmanaged remote access. The enforcement of security measures will be ensured and monitored through Active Defense & SIEM Implementation, which is necessary in order to detect any threats in the complex, outsourced cloud-based ecosystem. This SIEM-driven approach allows the implementation of a highly effective Compliance (GDPR) & Protection system for ensuring legal compliance, including encryption and breach reporting.

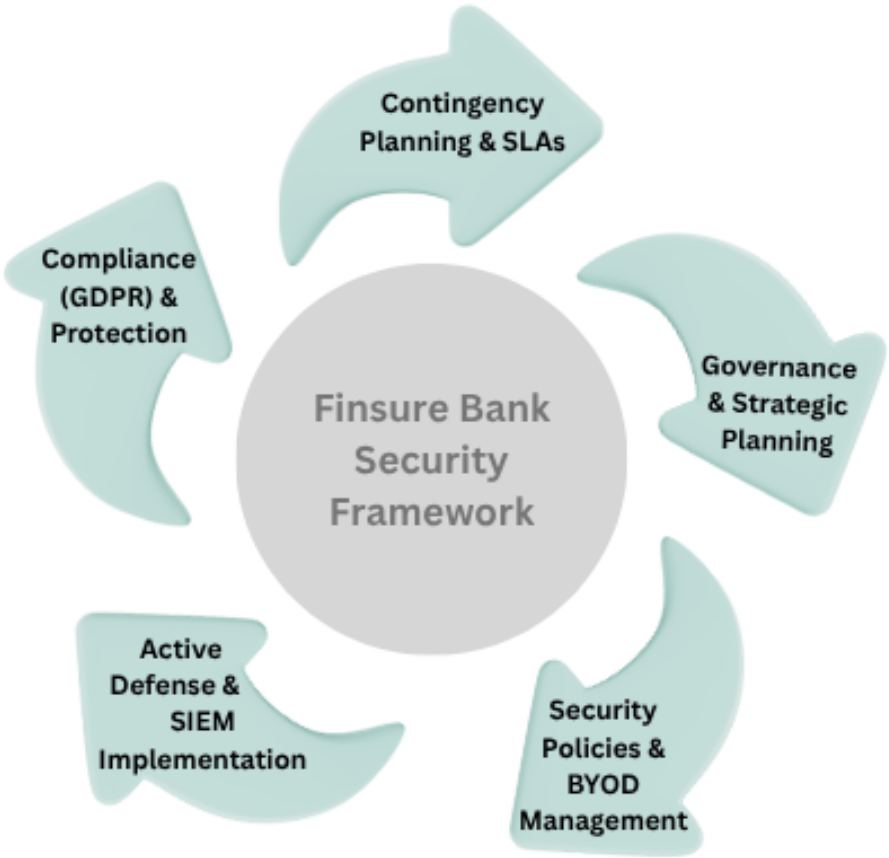

Figure 1: The FinSure Bank Security Framework Lifecycle

5.1 Governance and Strategic Planning

The concept of governance involves the degree to which security fits into the organization's wider business plans. The most pressing challenge for FinSure Bank is breaking up its fragmented security approach, one which poses great danger in its failure to have integrated risk management. In order to solve this issue, setting up the Information Security Steering Committee (ISSC) in a proper, formal manner is key. On the other hand, governance should not become an unnecessary barrier to agile operations in the digital age. Whereas the ISSC will be responsible for enforcing ISO/IEC 27001 accountability [1] and deciding on the overall risk tolerance, it is vital to strike the right balance between mandatory compliance and

agility. Planning for strategic initiatives should not depend on restrictive rules, but rather focus on developing a policy framework flexible enough to be enforced throughout the bank's 90 percent cloud ecosystem.

5.2 Security Policies & BYOD Risk Management

In light of tremendous pressure in operation, the firm adopts the Bring Your Own Device (BYOD) approach towards both their own personnel as well as their third-party contractors. Traditionally, security relied upon the notion of network perimeter protection. However, in a cloud-based environment, the concept of such perimeter protection no longer has any meaning. Hence, it becomes critically important to adopt Zero Trust Architecture (ZTA) [6] in order to avoid catastrophic breaches during access to financial information from a compromised endpoint. Moreover, ZTA operates under the assumption that all users on a corporate network pose a certain amount of risk to the company and hence needs to be verified. In light of BYOD challenges, it becomes critical to maintain a proper balance between organizational security measures and privacy concerns. The adoption of Mobile Device Management (MDM) solution could easily cause organizational conflict and potential litigation in courts of law due to its intrusiveness. Thus, it is better to use Mobile Application Management (MAM). Unlike MDM, MAM provides strong encryption-based data isolation of business data rather than seeking administrative control over the device.

5.3 Active Defense & SIEM Implementation

Despite the need for Zero Trust's important access controls, the company must implement proactive defense mechanisms. The highly distributed architecture and reliance on the cloud makes old-fashioned, perimeter-based firewalls wholly obsolete. Thus, SIEM becomes a requirement to manage vast telemetry data. One downside to SIEM technology is that it is prone to alert fatigue – analysts get swamped with thousands of false positives. As a solution to this, the aggregation of telemetry needs to be optimized. Using immutable Docker containers [7],

elasticity can be achieved to gather outside cloud telemetry while not impacting core banking applications' performance. Additionally, generic SIEM rule correlations do little to combat industry-specific cybercrimes. For this reason, the cybersecurity team needs to design custom heuristic algorithms through Python programming. Signature-based solutions were rendered obsolete years ago, as heuristics are based on behavior analysis that quickly spots suspicious behavior, such as impossible travel, and any off-hours BYOD use. Finally, any theoretical cybersecurity strategy requires extensive testing. Prior to implementing any new heuristics, experts need to ethically hack containers and correlate the attack telemetry with SIEM data.

5.4 Compliance (GDPR) & Protection Mechanisms

For FinSure Bank, which deals with highly sensitive financial and personally identifiable information (PII), there is a need to ensure that there is regulatory compliance. However, it is not possible to view regulatory compliance in a purely academic or theoretical sense. Rather, it is essential that there is deep operationalization of regulatory compliance using appropriate technical mechanisms. Being operational in both the UK and European markets binds the bank with the stringent legal requirements of the General Data Protection Regulation (GDPR) [3]. GDPR outlines the principles of integrity and confidentiality that necessitate that personal data is processed in a manner that is appropriate so that there is no unauthorized or unlawful processing, accidental loss, destruction, or damage.

To address these legal requirements in a highly distributed and 90% externally hosted cloud infrastructure, it is essential that the institution deploy robust cryptographic security measures. It is not acceptable to rely solely on the inherent security posture of the cloud infrastructure provider, which is in direct violation of the Shared Responsibility Model [4], which clearly states that the bank is ultimately legally liable to protect its customer data. As such, all databases and storage buckets in the cloud infrastructure will be required to implement mandatory encryption of data-at-rest using

the AES-256 encryption standard.

5.5 Contingency Planning and SLAs

In spite of this, the axiom of modern-day cybersecurity is that organizations are well-advised to assume a state of ultimate breach or systemic failure. As FinSure Bank is an organization that operates in a digital-first world in which over 90% of its infrastructure is externally hosted, it has, in effect, outsourced a massive portion of its operational availability risk to third-party Cloud Service Providers. In order to manage this outsourced risk, contingency planning and rigid Service Level Agreements are absolute imperatives.

An SLA is not only a technical document; it is also a legally enforceable governance contract that prescribes the acceptable parameters for the third-party relationship. It has to negotiate SLAs that ensure high availability, which is defined as achieving four nines (99.99%) up time for critical customer-facing banking applications. Moreover, the SLAs also need to be negotiated in such a manner that they define the MTTR in case of an outage and impose stringent financial penalties in case the CSP is unable to deliver on these parameters. However, from a strategic risk point of view, it is also important for the bank's steering committee to understand that, although financial penalties make the vendor culpable for non-performance, it does not mitigate the severe reputational damage and customer loss that a bank incurs in case of an outage.

Hence, relying solely on the SLA of the cloud service provider is not enough to mitigate the risk. Therefore, the bank must create its own Business Continuity Plan (BCP) and disaster recovery strategy, which must be tested regularly, following the guidelines of the relevant BCP standard, e.g., NIST SP 800-34 [9]. At the heart of the BCP and disaster recovery strategy is the determination of strict limits around two key variables: the Recovery Time Objective (RTO), which is the maximum time allowed for system downtime, and the Recovery Point Objective (RPO), which

determines the maximum acceptable threshold around data loss. For a financial institution where transactions are processed in real time, the RTO and RPO must be extremely low.

6. Critique of Dynamic Regulations and Standards

There needs to be careful scrutiny of why it is absolutely important for an organization to adopt the new or updated rules and regulations at all times. When it comes to corporate governance, one thing that poses a big risk is the fact that the people will perceive compliance as a static process. However, according to the diagram presented below, when organizations use static regulation processes, a regulatory lag is created. In other words, technology and cyber crime develop at such speed that they exceed the ability of the legislation to control them. To solve this problem and prevent the organizations from developing a false sense of security, regulatory frameworks should become more dynamic. The continuous process of updating rules and regulations is caused by three main things.

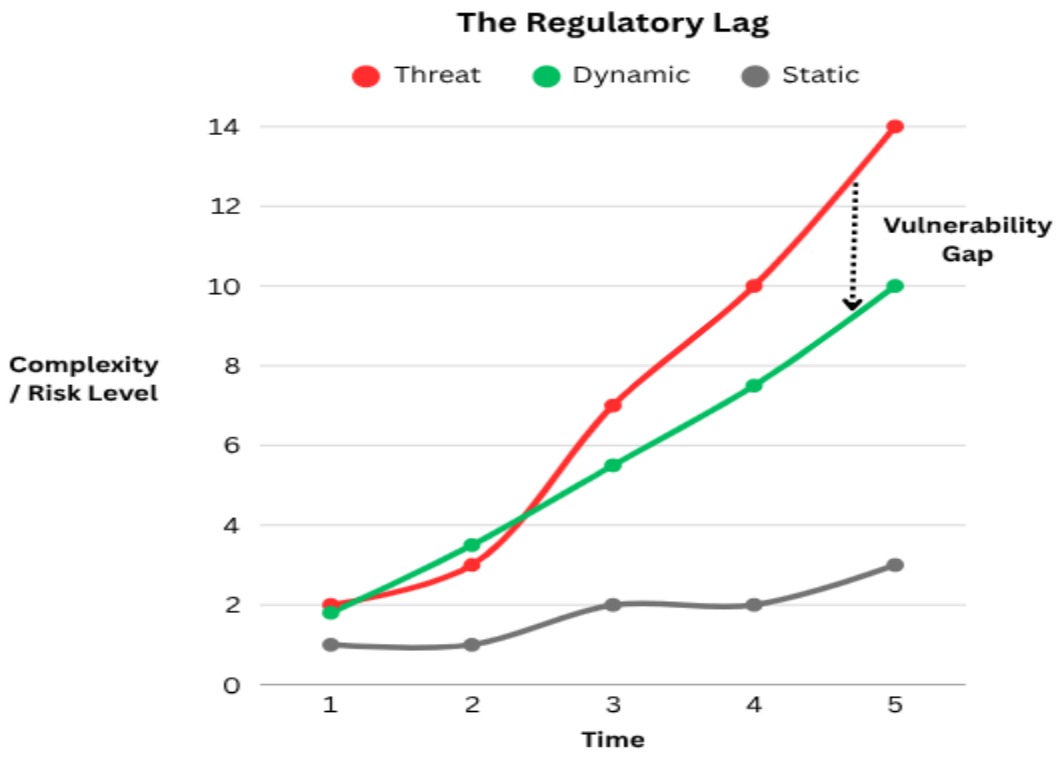

Figure 2: The Regulatory Lag - Static vs. Dynamic Frameworks

6.1. The Asymmetric and Evolving Threat Landscape

Cybercriminals are innovating continuously, using advanced resources to design new exploits, ransomware, and highly sophisticated Advanced Persistent Threats (APTs). Static regulations are outdated within a short period because they are designed to combat the threats that were known at the time of their formulation. For instance, regulations on data protection were designed to combat physical theft of documents or basic SQL injection attacks. Currently, attackers use Artificial Intelligence (AI) and Machine Learning (ML) to automate vulnerability scanning, making spear phishing attacks look extremely genuine. The dynamic changes to the ISO 27000 series [1] of regulations force organizations to continuously improve their defenses to combat the ever-changing, highly sophisticated threats, rather than the static threats of yesterday.

6.2 Fast Technological Innovations and Architectural Changes

The rate at which technology is evolving is much faster than the process of passing legislation, resulting in what is referred to as "regulatory lag" [10]. The widespread deployment of decentralized infrastructures, particularly multitenant cloud deployments and BYOD strategies, has exposed some significant vulnerabilities that were never considered in previous standards. In the event an organization relocates most of its resources externally, it means that the compliance measures put in place, especially those concerning physical location of data and limited perimeter access, become immediately outdated. Using static laws in the modern computing era creates major architecture loopholes. For this reason, dynamic regulatory policies are necessary. These policies ensure that any new technology being introduced into the organization is reviewed for security risks.

6.3 Ethical Responsibility and the Consumer's Right to Privacy

Moreover, the shift towards dynamic standards is necessitated by the need to address the ethics aspect. The more advanced financial institutions become in their techniques of processing consumers' data, the more they have to redefine ethical guidelines relating to privacy issues. Static guidelines often allow companies to take advantage of legislative gap for commercial gain through the exploitation of data. However, dynamic standards, which include strict interpretation of the UK GDPR [3] as well as extensive regulatory framework governing the consumers' rights [11], obligate companies to focus on users' preferences, data ownership, and transparency. Regulatory framework should evolve continuously to protect emerging consumers' rights like "Right to be Forgotten." Adherence to dynamic standards allows the organization to stay not only within the bounds of legislation but also fulfill ethical obligations of being a responsible keeper of sensitive data.

7. Conclusion

The quick evolution of FinSure Bank from being a local bank to a global, digitized organization has not only fueled massive growth but also created a series of security vulnerabilities that need to be mitigated immediately. The reliance on cloud services provided by external providers, in conjunction with the growing BYOD policy of the institution, has resulted in the dissolving of the company’s perimeters. These vulnerabilities place the enterprise at risk of insider threats, cybercrimes, and severe penalties due to lack of compliance with GDPR regulations.

In order to address the vulnerabilities described above, the recommendation made in this report is to make a strategic shift from a reactive IT policy towards an ISMS approach to information security. The adoption of international ISMS standards (ISO/IEC 27001), as well as ITIL best practices, would provide for a robust governance framework. This framework will help implement a Zero Trust Approach that requires constant authentication and authorization of users seeking access to BYOD devices.

In terms of practical engineering aspects, an important element that makes up the core of this approach to active defense involves implementation of a unique, highly optimized, and containerized SIEM system. Application of behavior-based alerts powered by Python code instead of generic alert mechanisms allows the bank's security specialists to identify and neutralize sophisticated threats on a proactive basis. Moreover, the use of this approach to active defense combined with mandatory application of encryption, automatic backups, and SLAs helps guarantee high system availability and full conformity with European regulations on data privacy. Thus, combining governance based on a particular theoretical framework with advanced SIEM solutions for active defense allows the bank to protect its assets and comply with applicable laws.

References

[1] International Organization for Standardization, "ISO/IEC 27001:2022 - Information security management systems," *ISO*, Oct. 2022. [Online]. Available: https://www.iso.org/standard/27001

[2] K. Kent and M. Souppaya, "Guide to Computer Security Log Management," *NIST Special Publication 800-92*, 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-92/final

[3] Information Commissioner's Office (ICO), "Guide to the UK General Data Protection Regulation (UK GDPR)," *ICO.org.uk*, 2023. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

[4] Amazon Web Services, "Shared Responsibility Model," *AWS Cloud Security*, 2023. [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/

[5] Axelos, "ITIL 4: High-velocity IT," *TSO (The Stationery Office)*, 2020. [Online]. Available: https://www.axelos.com/certifications/itil-service-management

[6] R. Ward and B. Beyer, "BeyondCorp: A New Approach to Enterprise Security," *login: The USENIX Magazine*, vol. 39, no. 6, pp. 6-11, Dec. 2014

.[Online]. Available: https://www.usenix.org/publications/login/december-2014/beyondcorp-new-approach-enterprise-security

[7] Docker Inc., "Docker Security," *Docker Documentation*, 2024. [Online]. Available: https://docs.docker.com/security/

[8] A. Kotenko, I. Saenko, and F. Skoruzpekin, "Analytical Visualization Techniques for Security Information and Event Management," *2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing*, 2013, pp. 522-526. [Online]. Available: https://ieeexplore.ieee.org/document/6498600/

[9] M. Swanson et al., "Contingency Planning Guide for Federal Information Systems," *NIST Special Publication 800-34 Rev. 1*, May 2010. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

[10] C. O'Brien, "Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers," *European Business Organization Law Review*, vol. 22, 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8294240/

[11] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer International Publishing, 2017. [Online]. Available: https://link.springer.com/book/10.1007/978-3-319-57959-7