การผนวกรวมตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไว้ในหน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบขององค์กร ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

The Integration of Data Protection Officer into the Compliance Team under the European Union's General Data Protection Regulation

สุภัทร์ ภู่พานิชเจริญกูล[1]
Suphat Phoophanichjaroenkul

บทคัดย่อ

บทความวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาวิเคราะห์ปัญหาทางกฎหมายตลอดจนความท้าทายอื่นเกี่ยวกับการผนวกรวมตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) ไว้ในหน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบขององค์กร (Compliance Department) โดยเฉพาะอย่างยิ่ง ความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้นเมื่อมีการกำหนดตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ในหน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบขององค์กร บทความวิจัยนี้เริ่มต้นด้วยการศึกษาข้อความคิดพื้นฐานและทฤษฎีเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection Regulation (GDPR) ซึ่งมีจุดมุ่งหมายในการปกป้องและคุ้มครองสิทธิความเป็นส่วนตัวของปัจเจกบุคคล บทความวิจัยนี้ศึกษาเปรียบเทียบบทบาทหน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและหน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบขององค์กร ภายใต้หลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense: 3 LoDs) ซึ่งกำหนดบทบาทและความรับผิดชอบของหน่วยงานให้เกิดการตรวจสอบและถ่วงดุลอำนาจ (Check & Balance) และบริหารความเสี่ยงที่อาจเกิดขึ้นภายในองค์กร บทความนี้วิเคราะห์ถึงประเด็นปัญหาเกี่ยวกับการขัดกันของผลประโยชน์ที่อาจเกิดขึ้นเมื่อมีการผนวกรวมตำแหน่งดังกล่าว บทกำหนดโทษตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ข้อห้ามตามกฎหมายที่ห้ามมิให้มีการเลิกจ้างหรือลงโทษเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตลอดจนการตรวจสอบถ่วงดุลระหว่างองคาพยพทั้งสอง ซึ่งต่างก็มีวัตถุประสงค์ภายในกรอบการกำกับดูแลที่แตกต่างกัน โดยเฉพาะหากมีการมอบหมายความรับผิดชอบเพิ่มเติมภายในหน่วยงานกำกับดูแล บทความวิจัยนี้เสนอแนวทางและมาตรการสำหรับองค์กรที่ต้องการผนวกรวมตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ในหน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบอย่างมีประสิทธิภาพ

คำสำคัญ: *การคุ้มครองข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล กฎหมายคุ้มครองข้อมูลส่วนบุคคล การปฏิบัติตาม*

---

[1]พนักงานคุมประพฤติปฏิบัติการ สำนักงานคุมประพฤติกรุงเทพมหานคร 11 กรมคุมประพฤติ กระทรวงยุติธรรม
Probation Officer, Practitioner Level, Bangkok Probation Office 11, Department of Probation, Ministry of Justice,
Corresponding author e-mail: suphatfu@gmail.com
ARTICLE HISTORY: Received 17 January 2024, Revised 23 September 2024, Accepted 31 May 2025

Abstract

This article explores the challenges associated with integrating Data Protection Officers (DPOs) within organizational frameworks, specifically addressing potential conflicts of interest that may arise when DPOs are positioned within the Compliance team. The study begins by introducing the overarching impact of the General Data Protection Regulation (GDPR), a pivotal legislative framework designed to safeguard individuals' privacy rights on a global scale. The research compares and contrasts the roles and responsibilities of DPOs and the Compliance function within organizations, elucidating their respective positions within the Three Lines of Defense Theory. The article analyzes various facets, including the potential conflicts of interest arising from integrating DPOs into the Compliance team. Special attention is given to the far-reaching implications of GDPR penalties and the regulatory mandate prohibiting the dismissal or penalty of DPOs. The study further examines the delicate balance required to avoid conflicting objectives within the regulatory framework, particularly when additional responsibilities are assigned within the Compliance team. In light of these analyses, the research proposes guidelines and measures for organizations seeking to navigate the complexities of DPO integration effectively.

Keywords: *Personal data protection, Data protection officer, GDPR, Compliance*

Introduction

Awareness in safeguarding personal data of individuals in European Union has emerged as a crucial determinant leading to the establishment of the General Data Protection Regulation (GDPR). The Council of the European Union enacted this regulation, which came into effect on 25 May 2018. The regulation places significant emphasis on the European Union's commitment to protecting the personal data of its citizens, as these rights are fundamental and have been consistently safeguarded since the inception of the European Union. Member States have adopted this regulation to ensure its efficacy within their respective jurisdictions, encompassing government agencies, private organizations, and independent entities. Furthermore, the impact of this regulation extends beyond the European Union, encompassing affiliates operating outside its borders. Consequently, the regulation exhibits global effectiveness and serves as a vital framework for non-European Union countries to adopt as a guide for enacting similar legislation within their own jurisdictions. The regulation also establishes essential principles instrumental in achieving its objectives, including the mandatory appointment of a data protection officer (DPO) by organizations operating under its purview.

DPOs play a pivotal role in serving as a nexus between data controllers, data processors, and data subjects, ensuring strict compliance with the regulation by both the data controller and the data processor. However, appointing a DPO poses challenges for organizations, particularly private companies. The responsibilities assigned to a DPO, such as monitoring the company's adherence to the regulation, bear resemblance to those of a company's compliance department. Consequently, the feasibility of incorporating a DPO within a company's compliance team becomes a critical consideration.

Objectives

The objectives of this study are as follows:

1. To examine the fundamental concepts and theories pertaining to the General Data Protection Regulation (GDPR) and its global impact on safeguarding individuals' privacy rights.
2. To compare and contrast the roles and responsibilities of Data Protection Officers (DPOs) and the Compliance function within organizations, with a specific focus on their positions in the Three Lines of Defense Theory.
3. To study and analyze the potential conflicts of interest that may arise when DPOs are integrated into the Compliance team, considering the impact of GDPR penalties, the prohibition of dismissal or penalty for DPOs, and competing objectives within the regulatory framework.
4. To propose appropriate guidelines and measures for organizations to ensure the effective integration of DPOs, emphasizing the need for independence in their roles and compliance with GDPR regulations.

Research Methodology

This study on the integration of Data Protection Officers (DPOs) within organizational compliance structures adopts a qualitative research approach, employing descriptive analysis methods. The methodology involves collecting primary sources, such as legal texts, through a documentary review, encompassing official documents like the General Data Protection Regulation (GDPR) text and regulatory guidelines. Secondary sources, including literature reviews, case studies, and document analysis of meeting minutes, newspaper articles, and reports from institutions, supplement the understanding of DPO roles and challenges. Internet research further gathers information on current trends and best practices. Utilizing descriptive analysis, this research aims to systematically examine the collected documents, offering a comprehensive understanding of DPO integration challenges and proposing guidelines for effective implementation within compliance structures.

Results

1. Emergence of the GDPR and Its Impact on Companies

The General Data Protection Regulation (GDPR) of the European Union has played a significant role in safeguarding individuals' privacy rights, which are fundamental principles of human rights both at the United Nations and European Union levels (Floridi. 2016). The GDPR's applicability extends beyond the European Union, impacting companies operating outside its jurisdiction due to the presence of numerous European companies worldwide (Freiherr von dem Bussche & Zeiter. 2016). Consequently, European companies operating in other regions are subject to the European Union's GDPR. Furthermore, the GDPR has served as a model for data protection laws in various countries, including Thailand's Personal Data Protection Act (Suwanprateep et al. 2022) and Singapore's Personal Data Protection Act (CMS Cameron McKenna Nabarro Olswang LLP. 2022). While these acts share similarities with the GDPR, they do not provide as detailed specifications.

Under the GDPR, data controllers and data processors are required to appoint data protection officers in three scenarios: when they are public bodies, when their main activities involve regular and systematic monitoring of personal information on a large scale, or when their main activities involve processing special categories of data (Danagher. 2012). Notably, even if the data controller and data processor are public bodies and do not engage in monitoring personal information or processing special categories of data, the appointment of a data protection officer remains mandatory.

It is worth noting that the role of data protection officers was also mentioned in the European Union Data Protection Directive 95/46/EC, which preceded the GDPR (The National Archives. 2022). Under the directive, any data controller or data processor was required to notify the supervisory authority before processing personal data, but the appointment of a data protection officer offered simplification or exemption from this obligation. [2]In other words, appointing a data protection officer was an alternative rather than a mandatory compliance requirement under the previous regulation. However, the current GDPR mandates private sector entities that meet the specified criteria to appoint a data protection officer within their organizations.

---

[1]Data Protection Directive 95/46/EC Article 18

[2]Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, ..."

2. Roles and Responsibilities of the Compliance Function and Data Protection Officer

The Basel Committee has provided a definition for compliance risk, stating that it encompasses the potential legal or regulatory penalties, financial losses, or reputational damage a bank may face due to non-compliance with applicable laws, regulations, codes of conduct, and good practice standards (Bank for International Settlements. 2022). The Compliance team holds key responsibilities in managing various risks within the company, including regulatory risks, credit risk, market risk, operational risk, and strategic risk (Fahrul & Rusliati. 2016). These responsibilities encompass providing guidelines and policies for compliance risk management, regular reporting on the adequacy of compliance governance, identification and assessment of compliance risks, notification of compliance issues and violations to top management, and supporting other departments, particularly the Risk Management Department, in preparing reports on operational and reputational risks (Misha. 2016). Failure to effectively address these risks may lead to damage to the firm's reputation.

Turning to the duties of a Data Protection Officer (DPO), as outlined in Article 39 of the General Data Protection Regulation (GDPR), the DPO is tasked with informing and advising the data controller, processor, and employees involved in processing operations. The DPO also monitors compliance with the GDPR, including assigning responsibilities, raising awareness, providing training, conducting audits, offering advice on data protection impact assessments, cooperating with supervisory authorities, and serving as the contact point for such authorities.[3]

Considering the inherent differences between these positions, integrating the role of a DPO into a company's Compliance team presents challenges. However, such an approach warrants consideration as it can centralize responsibilities within the Compliance team, facilitating departmental management and preserving the company's human resources (Table 1).

[3]General Data Protection Regulation, Article 39

Table 1: Comparing the Roles of Data Protection Officer and Compliance Officer

Functions	Data Protection Officer	Compliance Officer
Differences		
Scope of Focus	Primarily focused on GDPR and other data protection laws. Their role is specialized in ensuring data protection compliance.	Manages compliance across multiple regulatory frameworks, which might include GDPR but also covers areas like financial regulations, environmental laws, etc.
Independence	Must act independently to fulfill their duties, with direct reporting lines to top management or the board to avoid conflicts of interest.	While expected to act ethically, they are often integrated within the operational structure, reporting through legal or risk management departments.
Decision-Making Authority	Has the authority to halt or challenge data processing activities that violate GDPR, acting as a guardian of data privacy	Implements compliance policies but might not have the same level of authority to unilaterally stop operations unless it's a clear violation of multiple regulations.
Risk Assessment	Specifically focuses on data protection risks, often through Data Protection Impact Assessments (GDPR Article 39)	Manages risks across all compliance areas, which might include data protection but is not exclusively focused on it.
Training and Awareness	Conducts training specifically related to data protection laws and practices.	Provides training on a broader spectrum of compliance issues, including but not limited to data protection.
Similarities		
Regulatory Compliance	Both roles aim to ensure the organization complies with applicable laws, albeit with different focuses.	
Policy Development	Both are involved in creating and updating policies, though the DPO's policies are centered around data protection.	
Monitoring and Reporting	Both roles monitor compliance activities and report to higher management or external bodies (for DPOs, this includes supervisory authorities).	
Training and Education	Both engage in educating employees about compliance, though the content and focus differ.	
Risk Management	Both assess and manage risks, with the DPO focusing on data protection risks and the Compliance Officer on broader operational and regulatory risks.	
Stakeholder	Both interact with various stakeholders, though the DPO's engagement often involves data subjects and data protection authorities more directly.	

3. Position of the Data Protection Officer in the Three Lines of Defense Theory

When analyzing the positions and responsibilities of the data protection officer and the compliance officer, it becomes evident that certain similarities exist. Both roles share the duty of overseeing the firm's adherence to regulatory requirements in order to mitigate compliance risk. However, it is important to consider the three lines of defense framework, which divides risk management into accountability in the first line, independent challenge in the second line, and assurance and review in the third line (Daisley *et al.* 2022).

The three lines of defense structure entails separate internal audits for each line: risk identification in the first line, the internal audit and control system in the second line, and an independent system ensuring the accuracy of the internal audit system in the third line (Mrsik, Nenovski, & Dimov. 2017). The Federation of European Risk Management Associations (2022a) highlights the significance of the three lines of defense framework in helping company management understand the crucial role of internal auditing in overall risk management. This model is applicable to public, private, and non-profit organizations.

Considering the positions of the compliance officer and the data protection officer, both are situated in the second line of defense according to the instructions of the Federation of European Risk Management Associations (2022b) and the European Banking Authority (2022). These guidelines stipulate that data protection officers should possess neutral and independent qualifications separate from personal data processing activities. However, such recommendations may inadvertently obscure the distinct roles of data protection officers, much like the compliance officer's position.

Nevertheless, the effectiveness of the three lines of defense model remains a subject of debate. The classification of lines is not always definitive, and the model is often more theoretical than practical. This model has the potential to diffuse risk responsibilities, reducing transparency instead of enhancing it (Davies & Zhivitskaya. 2018). Additionally, Ernst and Young (2022) argue that the efficiency of the model remains unclear, as it fails to provide a comprehensive mapping of risks within each line.

Considering these arguments, placing the data protection officer within the second line of defense may not be entirely reliable. Article 39 of the General Data Protection Regulation primarily focuses on the operational governance of data processing, rather than examining whether the control and processing of data by the company comply with the regulation. Data protection officers are solely responsible for monitoring and possess independence in performing their duties, separate from the compliance

officers. Therefore, it is advisable to position the data protection officer in a different line than the compliance function.

Discussion

1. Conflict of interest

The Data Protection Officer (DPO) may be an individual whose scope of work is solely related to data protection, or it can be someone within the organization who assumes this role alongside other responsibilities. Additionally, the DPO does not necessarily have to be an employee of the organization, as companies have the option to outsource this function to a third party (Information Commissioner's Office. 2022b).

Under the General Data Protection Regulation (GDPR), companies are not obligated to appoint a dedicated DPO. However, the company can assign additional tasks to the DPO as long as it does not compromise the DPO's primary duty. Article 38(6) of the GDPR allows the DPO to perform other duties, provided that it does not impact their independence and ability to monitor compliance without any conflicts of interest.[4]

Compared to the previous regulation, the European Union Data Protection Directive (Directive 95/46/EC), the GDPR has increased the company's duty to appoint a DPO. Previously, the appointment of a DPO was merely optional under the Data Protection Directive. Although the Data Protection Directive specified that the company must enable the DPO to perform their duties independently[5] , there were no penalties for non-compliance.

In contrast, the current GDPR clearly states penalties[6], which can be as high as 20 million Euros or 4 percent of worldwide gross revenues (Hintze & LaFever. 2017). As De Hert and Papakonstantinou (2012) pointed out, the appointment of a DPO may be viewed as burdensome by companies that were not previously required to appoint one. However, in the draft of the GDPR (PDC Informatie Architectuur. 2022), specific criteria were outlined for the appointment of DPOs, such as having expertise in data processing and a company size of at least 250 employees (Reding. 2012). Subsequently, the requirement regarding the number of company employees was adjusted to reduce the burden, particularly for small and medium-sized enterprises (SMEs) (Voss, 2016). This effort aimed to ensure compliance with the regulation only for companies with significant data processing activities.

---

[4]General Data Protection Regulation, Article 38 (6)

[5]European Union Data Protection Directive (Directive 95/46/EC), Recital 49

[6]General Data Protection Regulation, Article 83

The GDPR does not prohibit DPOs from performing other duties, but it is crucial to weigh the burden on the company against the DPO's independence in carrying out their duties without interference. A recent ruling by the Bavarian Data Protection Authority ("BayLDA") sheds light on the appointment of a DPO, emphasizing the importance of reliability and independence in the DPO's role to ensure compliance with the GDPR (Kaufmann & Guenther. 2022b). The BayLDA deemed it a conflict of interest when the Data Protection Officer's role was merged with that of the company's Information Technology Manager. As a DPO, the individual must objectively control their own actions as an Information Technology Manager to ensure compliance with data protection laws. The BayLDA requested the appointment of a separate DPO to ensure compliance, and failure to comply resulted in a fine for the company.

Although BayLDA's decision is based on German Data Protection law, which shares the same content as the European Union GDPR, it is essential to note that enforcement of the regulation should be consistent. From the report, it is evident that conflicts of interest can arise if the DPO holds other positions within the company, such as the head of departments like Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, Chief Medical Officer, Head of Marketing, Head of Human Resources, or Head of IT (Kaufmann & Guenther. 2022a). Such individuals heavily involved in the processing of personal customer information are not suitable candidates for the role of DPO.

Turning to the duties of the compliance department, compliance officers perform various functions depending on the nature of the organization's business. When considering whether appointing a DPO within the compliance department would create a conflict of interest, it is necessary to determine if the data used in the process qualifies as personal data under the GDPR. Moreover, if the activity involves the processing of personal data, it includes not only customer data but also employee data.

For instance, in the case of financial institutions, the compliance department's responsibility is to investigate financial crimes, mitigate the organization's risk of financial offenses, combat money laundering, counter terrorist financing, prevent bribery and corruption, and ensure adherence to regulatory standards at international and national levels. Compliance officers monitor customer personal data to verify customer identification information (PWC. 2022).[7]

---

[7]Customer identification information, as follows ;

Based on the information above, such customer information falls within the definition of 'personal data' under Article 4 of the GDPR.[8] Additionally, compliance functions need to ensure that transactions are not involved in money laundering, terrorist financing, or corruption related to Politically Exposed Persons (PEPs). The compliance team is obligated to provide Suspicious Transaction Reports (STRs) and submit them to the supervisory authority. These data are considered personal data according to the definition provided in Article 4(1) of the GDPR.

For individuals: full name, home address and birth date ideally from a government-issued document that includes a full name and photo of the customer, and either residential address or date of birth e.g. valid passport, valid photocard driving license etc ; or a government-issued document (without a photograph) that includes the full name of the customer, backed up by a second document; either a government issued or issued by a judicial body, a public sector body or authority, a regulated utility company, or another FSA regulated company in the UK financial services industry or equivalent jurisdiction, including the full name of the customer and either the residential address or the date of birth.

For companies: full name, registration number, country of incorporation registered office, company address. In addition, for private/unlisted companies: names of all directors (or equivalents), names of individuals who own or control more than 25% of their shares or voting rights, and names of individuals who otherwise exercise control over the company's management. The company should verify the existence of the company either by confirming the listing of the company on a regulated market or by searching the relevant company registry or by copying the company's Certificate of Incorporation. After a risk assessment, companies may decide to verify one or more directors as appropriate in accordance with CDD requirements for private / unlisted companies for individuals. With respect to Beneficial owners, the company must take risk-based and appropriate measures to verify the Beneficial Owner's identity.

Furthermore, if the compliance officer needs to monitor the disclosure of personal data of the company's employees, such as when the company is a financial institution requiring employees to disclose personal trading accounts and outside business benefits to prevent conflicts of interest (Financial Conduct Authority, 2022a), or such as individual investment accounts and affiliates, including shares in public companies and private investments, that information also qualifies as personal data under the GDPR.

---

[8]General Data Protection Regulation, Article 4(1)

It is evident that the compliance team acts as a personal data processor, and as such, they must comply with the GDPR. In cases where the data controller or data processor fails to comply with the GDPR or engages in actions that conflict with the regulation, the DPO is responsible for providing advice or informing the data controller or data processor about their non-compliance or actions that violate the regulation.[9]

Therefore, if the DPO and compliance officer are the same person or embedded within the same function, it would create a conflict of interest for the DPO to assess whether their actions comply with the GDPR. This conflict of interest contradicts the requirements of the GDPR and may result in penalties for the company.

In the context of financial institutions, compliance officers have a responsibility to comply with the Bank for International Settlements (BIS) Compliance Charter, ensuring the performance of their duties independently and being accountable (Bank for International Settlements, 2022). The compliance officer should not be placed in a position that could lead to a potential conflict between their compliance duties and other responsibilities. Additionally, the BIS Compliance Charter requires that if compliance officers are assigned duties unrelated to compliance, they must report directly to the Chief Compliance Officer. This requirement contradicts the GDPR, which mandates that the DPO reports directly to the top management of the organization.[10]

In healthcare, the handling of personal data, especially health data, is highly sensitive due to its intimate nature and the potential for severe harm if mishandled. Healthcare organizations must comply with GDPR's stipulations on special categories of data, which include health data. The integration of a Data Protection Officer in healthcare aims to ensure that all data processing activities, from patient records to clinical research, adhere to privacy laws. This involves managing consent, ensuring data security, and facilitating patient rights like access to their health data (Metomic. 2024; DPOcentre. 2024).

In the insurance sector, data protection compliance focuses on customer data used for underwriting, claims processing, and risk assessment. Insurance companies process vast amounts of personal data, often involving sensitive information like financial status or health conditions. The DPO in insurance companies must ensure that data practices comply with GDPR, especially when dealing with international data

---

[9]General Data Protection Regulation, Article 39(a)-(b)

[10]General Data Protection Regulation, Article 38(3)

transfers or third-party data processors. The role involves overseeing data protection impact assessments, ensuring proper data encryption, and managing data breaches, all while aligning with the strategic business goals of risk assessment and policy pricing (InCountry. 2024).

At the EU level, the European Securities and Markets Authority (ESMA) has established guidelines that assign responsibilities to investment companies, ensuring independence in compliance functions (European Securities and Markets Authority. 2022). Furthermore, in the Senior Management Arrangements, Systems and Controls (SYSC) framework established by the Financial Conduct Authority (FCA) for overseeing financial institutions in the United Kingdom, SYSC 6.1.3 (Financial Conduct Authority, 2022b) stipulates that companies must ensure compliance officers can perform their duties independently and efficiently without interference. Failure to comply with these rules and regulations may result in penalties from the FCA for non-compliance.

Therefore, it is the company's responsibility to ensure that conflicts of interest between the DPO and compliance officer are avoided, allowing them to carry out their duties independently without interference from other departments.

2. No Instruction, Dismissal, or Penalty by the Data Controller or Data Processor

Another aspect to consider is outlined in Section 38(6), which demonstrates that conflicts of interest extend beyond the previously mentioned scenario. It encompasses factors that may hinder the Data Protection Officer (DPO) from making independent decisions due to certain responsibilities or repercussions. Specifically, the Compliance Officer bears direct responsibility for ensuring the firm's compliance with the General Data Protection Regulation (GDPR), while the DPO is not personally accountable for non-compliance.

In accordance with the regulation, only the data controllers and data processors are held responsible for such cases, as stated in Article 83(3). Notably, the DPO is not personally liable, and Article 38(3) prohibits the dismissal or penalization of DPOs by data controllers and data processors. However, if the compliance officer and DPO are the same individual or occupy the same role, it may impede the freedom of decision-making. As a data processor, the compliance officer still carries liability and may be subject to penalties under the GDPR or other regulatory provisions. Consequently, the DPO may factor in such liability when making decisions.

Section 38 (3) mandates that the DPO be able to work independently without receiving guidance regarding their duties. Although the regulation does not explicitly prohibit any individual from being involved with the DPO, it emphasizes that data controllers, data processors, other personnel within the company, or any other factors

must not exert influence over the DPO's decision-making process when performing their duties.

Additionally, the DPO is required to provide advice and guidance to data controllers and data processors to enhance operational processes in accordance with the GDPR. Placing the DPO within the compliance team raises concerns as it may give the impression that the DPO is advising and guiding themselves.

3. Competing Objectives

However, it is essential to consider whether the information being used qualifies as personal data and whether the activity involves the processing of such information. In certain instances, the compliance team may not have the obligation to process personal data at all, such as when conducting employee training to educate them on the company's rules and regulations to ensure proper adherence. In this scenario, it is evident that the training does not involve the processing of personal data.

Employee training is a routine task assigned to compliance officers to educate relevant employees. In such cases, it may seem appropriate to delegate this responsibility to data protection officers. However, despite the absence of apparent conflicts of interest, the primary objective of the General Data Protection Regulation (GDPR) is to ensure that data protection officers perform their duties fully and efficiently, without any mitigating factors.

This has prompted the Information Commissioner's Office (ICO) to issue recommendations clarifying that "DPOs should not be expected to manage competing objectives that could undermine the primacy of data protection in favor of business interests" (Information Commissioner's Office. 2022a). Therefore, the compliance department must take into account that assigning additional functions to the data protection officer will inevitably result in their primary role, as stipulated by the GDPR, being diminished to a secondary role.

Conclusion

In conclusion, the integration of data protection officers within the compliance department leads to various adverse consequences. The roles and responsibilities of data protection officers and compliance officers inherently involve conflicts of interest, as the compliance officer, acting as a data processor, ends up assessing their own actions. Furthermore, when it comes to liability under the regulations, the data protection officer is explicitly exempted from personal liability, ensuring the independence of their role. On the other hand, the compliance officer remains a data processor and

retains responsibilities as dictated by the regulations. The integration of these positions may compromise the decision-making process. Even if non-data processing tasks are assigned to the data protection officer, it can significantly diminish their primary role of safeguarding personal information. Ultimately, the integration of these positions may expose the company to legal liabilities under the General Data Protection Regulation and other relevant laws, as outlined above.

For further exploration, a global comparative analysis is recommended to understand how different countries and regions approach the integration of DPOs within organizational structures. This study can offer insights into diverse regulatory frameworks and their impact on organizational practices, providing a broader understanding of global trends. Investigating employee perceptions and attitudes towards DPO integration within Compliance teams is another avenue for further study. Exploring the integration of technological solutions to streamline the roles of DPOs and Compliance functions is also recommended. Assessing the impact of emerging technologies, such as artificial intelligence and automation, on data protection processes and compliance outcomes can offer valuable insights.

Suggestions

The role of a Data Protection Officer (DPO) as outlined by Article 39 of the GDPR involves several key responsibilities that are distinctly focused on data protection. The DPO is tasked with informing and advising the organization and its employees on their obligations under the GDPR, ensuring that everyone within the organization understands the implications of data protection laws. This advisory role extends to monitoring compliance with both GDPR and other data protection provisions, where the DPO ensures that the organization's data protection policies are not only in place but are also followed rigorously. Moreover, when it comes to high-risk data processing activities, the DPO provides crucial advice on Data Protection Impact Assessments (DPIAs) and monitors their implementation. This role is not just about compliance but about proactively assessing and mitigating risks associated with data processing. The DPO also serves as the primary contact for supervisory authorities, facilitating communication and cooperation, which is a specialized function not typically within the remit of general compliance officers.

The distinction between the DPO's tasks and those of compliance officers lies primarily in scope, independence, and focus. Compliance officers often manage a wide array of regulatory requirements, where GDPR compliance might be one aspect among many. Their role involves operational compliance, training, and policy implementation across various regulatory domains. In contrast, the DPO's expertise is concentrated

on data protection laws, ensuring their independence to perform their duties without internal pressures that might compromise data protection. While both roles might engage in training and policy development, the DPO's advisory capacity is more strategic, focusing on the legal interpretation and application of data protection laws rather than the broader operational compliance managed by compliance officers. This strategic advisory role of the DPO includes not only internal guidance but also external engagement with supervisory authorities, acting as the organization's face for GDPR-related matters. Furthermore, the DPO's involvement in risk assessment, particularly through DPIAs, underscores a specialized approach to understanding and mitigating risks associated with data processing operations, which might not be as detailed or specialized in the broader compliance role. This legal versus operational compliance distinction ensures that while there might be overlaps, the DPO's role provides a dedicated, expert approach to GDPR compliance, maintaining the necessary independence and focus on data protection governance. This clarity in roles helps organizations not only in adhering to regulatory requirements but also in safeguarding the integrity of their data protection practices.

To effectively integrate Data Protection Officers (DPOs) within organizational compliance structures while maintaining their independence and effectiveness, several key guidelines and measures should be considered. Firstly, it's crucial to establish a clear definition of the DPO's role, ensuring that their responsibilities are strictly aligned with GDPR Article 39 without any additional conflicting duties. This role should be distinctly separated from positions that might lead to conflicts of interest, such as those involved in decision-making on data processing activities. Structural independence is paramount for DPOs as well. They should report directly to the highest level of management, ideally the board of directors, to avoid undue influence from middle management. This direct line of communication ensures that the DPO can perform their duties without compromise. Additionally, organizations must guarantee that DPOs are not dismissed or penalized for carrying out their responsibilities, reinforcing their independence. Organizations should provide the DPO with adequate support, including sufficient staff, budget, and access to necessary data and operations. Continuous professional development is also essential to keep the DPO updated on evolving data protection laws and practices.

Operational measures need to include a robust conflict of interest policy, preventing the DPO from holding positions where their impartiality could be questioned. Regular audits and reviews should be conducted to ensure the DPO is fulfilling their role without interference, maintaining the integrity of data protection practices within the organization. Engagement with supervisory authorities should be facilitated by al-

lowing the DPO the autonomy to communicate freely without needing prior approval from higher management. This ensures that the organization's data protection practices are transparent and compliant with external regulatory expectations. Also, cultural integration involves running organization-wide awareness programs to educate all employees on the importance of data protection and the DPO's role, fostering a culture of privacy. Establishing mechanisms for employees to report data protection concerns directly to the DPO, with protections against retaliation, can also enhance this culture. Plus, documentation and accountability are critical areas where the DPO should oversee the maintenance of detailed records of all data processing activities, ensuring GDPR compliance. Their involvement in Data Protection Impact Assessments (DPIAs) from the outset is vital, ensuring that data protection considerations are integral to decision-making processes.

Finally, periodic reviews of the DPO's position and effectiveness within the organization are necessary to adapt to new regulations, technologies, or business practices. A formal feedback mechanism should be in place for the DPO to provide direct feedback on data protection practices to the organization's governing body.

In addition to these measures, advocating for comprehensive training programs for both DPOs and compliance teams can enhance their understanding of GDPR and other relevant legal frameworks, promoting effective collaboration while maintaining distinct roles. Emphasizing the DPO's independence through measures like direct reporting lines to top management, rather than within the compliance team, is crucial. Regular audits and assessments should be recommended to evaluate the effectiveness of DPO integration, ensuring that data protection practices remain robust and compliant. By implementing these guidelines, organizations can foster an environment where the DPO operates effectively, maintaining independence while collaborating with compliance teams to uphold data protection standards, thereby ensuring compliance with GDPR and enhancing organizational integrity and trust in data handling practices.

References

Article 29 Data Protection Working Party. (2022). **'Guidelines On Data Protection Officers ('Dpos'). Ec.europa.eu.** Retrieved 15 May 2022, from https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

Bank for International Settlements. (2022A). **BIS Compliance Charter.** Retrieved 18 May 2022, from https://www.bis.org/about/compliancecharter.pdf.

Bank for International Settlements. (2022B). **Compliance and the Compliance Function in Banks.** Retrieved 18 May 2022, from https://www.bis.org/publ/bcbs113.pdf.

CMS Cameron McKenna Nabarro Olswang LLP. (2022). **A Guide to GDPR For Companies in Singapore.** Retrieved 18 May 2022, from https://cms.law/en/media/affiliates/singapore/images/publications/gdpr-guide-for-singapore-companies.

Daisley, M., McGuire, S., Netherton, G., & Abrahamson, M. (2022). **Whose Line Is It Anyway? Defending the Three Lines of Defence.** Oliverwyman.com. Retrieved 18 May 2022, from https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/nov/LON-MKT10304-010-Three-lines-of-defence-PoV-FINAL.PDF.

Danagher, L. (2022). **An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?** Ejlt.org. Retrieved 18 May 2022, from https://ejlt.org/index.php/ejlt/article/view/171.

Davies, H., & Zhivitskaya, M. (2018). Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? **Global Policy.** 9: 34-42.

De Hert, P., & Papakonstantinou, V. (2012). The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals. **Computer Law & Security Review.** 28(2): 130-142.

DPOcentre. (2024). GDPR, **Data Protection for Medical & Healthcare.** Retrieved 19 September 2024, from https://www.dpocentre.com/sector/healthcare/.

Ernst and Young. (2022). **Maximizing Value from Your Lines of Defense a Pragmatic Approach to Establishing and Optimizing Your LOD Model.** Retrieved 18 May 2022, from https://www.iia.nl/SiteFiles/EY-Maximizing-value-from-your-lines-of-defense.pdf.

European Banking Authority. (2022). **Compliance Function and Anti-Money Laundering tasks, Data Protection Officer or FATCA&CRS Responsible Officer, and Fraud Management - European Banking Authority.** Retrieved 18 May 2022, from https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_3956.

European Securities and Markets Authority. (2022). **Guidelines on Certain Aspects of the Mifid Compliance Function Requirements.** Esma.europa.eu. Retrieved 23 May 2022, from https://www.esma.europa.eu/sites/default/files/library/2015/11/2012-388_en.pdf.

Fahrul, M., & Rusliati, E. (2016). Credit Risk, Market Risk, Operational Risk and Liquidity Risk on Profitability of Banks in Indonesia. **TRIKONOMIKA.** 15(2): 78-88.

Federation of European Risk Management Associations. (2022a). **Audit and Risk Committees News from EU Legislation and Best Practices'.** Retrieved 23 May 2022, from https://www.ferma.eu/app/uploads/2014/10/ECIIA_FERMA_Brochure_v8.pdf.

Federation of European Risk Management Associations. (2022b). **FERMA'S Views on the Guidelines on Data Protection Officers Adopted on 13 December 2016 by the Article 29 Data Protection Working Party 15 February 2017.** Retrieved 23 May 2022, from https://www.ferma.eu/app/uploads/2019/02/ferma-comments-dpo-guidelines-art-29-working-party.pdf.

Financial Conduct Authority. (2022a). **'New Conduct of Business Sourcebook Chapter 11 Dealing and Managing.** Retrieved 23 May 2022, fromhttps://www.handbook.fca.org.uk/handbook/COBS/11/7.pdf.

Financial Conduct Authority. (2022b). **SYSC 6.1 Compliance - FCA Handbook.** Handbook.fca.org.uk. Retrieved 23 May 2022, from https://www.handbook.fca.org.uk/handbook/SYSC/6/1.html.

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. **Philosophy & Technology,** 29(4): 307-312.

Freiherr von dem Bussche, A., & Zeiter, A. (2016). Practitioner's Corner "Implementing the EU General Data Protection Regulation: A Business Perspective. **European Data Protection Law Review,** 2(4): 576-581.

Hintze, M., & LaFever, G. (2017). Meeting Upcoming GDPR Requirements While Maximizing the Full Value of Data Analytics. **SSRN Electronic Journal.** https://doi.org/10.2139/ssrn.2927540

InCountry. (2024). **Data Protection Principles in the Insurance Industry.** InCountry.com. Retrieved 23 April 2024, from https://incountry.com/blog/data-protection-principles-in-the-insurance-industry/.

Information Commissioner's Office. (2022a). **Data Protection Officers.** Retrieved 23 May 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/.

Information Commissioner's Office. (2022b). **Guide to the General Data Protection Regulation (GDPR).** Retrieved 23 May 2022, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

Kaufmann, J., & Guenther, J. (2022a). Data Protection Officers Must Not Have a Conflict of Interest – Part 2. **Global Compliance News.** Retrieved 23 May 2022, from https://globalcompliancenews.com/data-protection-officers-conflict-interest-20180109.

Kaufmann, J., & Guenther, J. (2022b). Germany: Data Protection Officer Must Not Have a Conflict of Interests. **Global Compliance News.** Retrieved 23 May 2022, from https://globalcompliancenews.com/germany-data-protection-officer-conflict-of-interest-20161121.

Metomic. (2024). **How Does GDPR Apply to Healthcare Organisations?** Retrieved 19 September 2024, from https://www.metomic.io/resource-centre/how-does-gdpr-apply-to-healthcare-organisations

Misha, Av. Ergys. (2016). "The Compliance Function in Banks and the Need for Increasing and Strengthening its Role - Lessons Learned from Practice". **European Journal of Sustainable Development.** 5(2): 171-180.

Mrsik, J., Nenovski, T., & Dimov, A. (2017). The Three Line of Defence Model for Effective Risk Management in Local Government. **Economic Development/ Ekonomiski Razvoj.** 19(3): 153.

PDC Informatie Architectuur. (2022). **Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).** Retrieved 18 May 2022, from https://www.eumonitor.eu/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vjvh54kbamzv/f=/10391_15.pdf.

PWC. (2022). **'Know Your Customer: Quick Reference Guide Understanding Global KYC Differences.** Retrieved 23 May 2022, from https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-anti-money-laundering-2016.pdf.

Reding, V. (2012). The European Data Protection Framework for the Twenty-first Century. **International Data Privacy Law.** 2(3): 119-129.

Suwanprateep, D., Paiboon, P., Buranatrevedhya, K., & Yanprasart, J. (2022). The First Thailand Personal Data Protection Act Has Been Passed. **Global Compliance News.** Retrieved 18 May 2022, from https://www.globalcompliancenews.com/2019/03/06/first-thailand-personal-data-protection-act-has-been-passed-20190401/.

The National Archives. (2022). **Directive 95/46/EC of the European Parliament and of the Council.** Retrieved 18 May 2022, from https://www.legislation.gov.uk/eudr/1995/46/pdfs/eudr_19950046_adopted_en.pdf.

Voss, W. G. (2016). Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation. **Revue juridique Thémis de l'Université de Montréal.** 50 (3): 783-820.