LAPPEENRANTA-LAHTI UNIVERSITY OF TECHNOLOGY LUT
School of Engineering Science
Software Engineering
Master's Programme in Software Engineering and Digital Transformation

Taiwo Bamigbala

DATA ETHICS AND NON-COMPLIANCE CHALLENGES IN DEVOPS

Examiners : Associate Professor Antti Knutas
Associate Professor Annika Wolff

Supervisors: Associate Professor Antti Knutas
Associate Professor Annika Wolff

ABSTRACT

Lappeenranta-Lahti University of Technology
School of Engineering Science
Software Engineering
Master's Programme in Software Engineering and Digital Transformation

Taiwo Bamigbala

Data Ethics and Non-compliance Challenges in DevOps

Master’s Thesis 2023

80 pages, 5 figures, 11 tables and 1 appendix

Examiners: Associate Professor Antti Knutas
Associate Professor Annika Wolff

Keywords: DevOps, Data Ethics, Compliance, Regulation, Framework, Privacy, Controls

Competition in the global marketplace has continued to drive the need for faster development and release of software applications as well as easier maintenance of existing ones. DevOps as a software development methodology enables these possibilities by bridging the communication and collaboration gap that often exist between traditionally independent development and operations team. This report aims to identify and investigate factors that can affect data ethics; the moral obligation of collecting, protecting, and using personal data within the DevOps environment. The research was conducted using non-systematic literature review of past works and semi-structured interview. The result of the semi-structured interview was analysed using thematic analysis while a process model for implementation of Data Ethics framework in DevOps is developed based on design science research method. The research identifies organisational culture, size of organisation, lack of automated tools to detect data ethical breaches and inadequate training & awareness as some of the responsible factors. Mitigation and improvement strategies especially on DevOps personnel trainings and implementation of a Data governance framework is provided in the report.

ACKNOWLEDGEMENTS

This thesis has greatly expanded my knowledge on Data Ethics within the DevOps practice. My sincere gratitude to my supervisors for their patience and commitment towards the success of this project. I also appreciate my family for providing me with emotional support while working on this thesis.

Table of Contents

Appendices

Appendix 1. Transcribed Interview data

LIST OF SYMBOLS AND ABBREVIATIONS

SDLC	Software Development Life Cycle
DevOps	Development & Operations
HIPAA	Health Insurance Portability and Accountability Act
GDPR	General Data Protection Regulation
ISO	International organization for standardization
DSRM	Design science research methodology
NSR	Non systematic review
DPR	Data Protection Act
IEEE	Institute of Electrical and Electronics Engineers
TA	Thematic Analysis
IT	Information Technology
CICD	Continuous Integration Continuous Delivery
QA	Quality Assurance
RQ	Research Question
DLP	Data Loss Prevention
KPI	Key Performance Indicator

1 INTRODUCTION

1.1 Background

The paradigm shifts of organisations from manual information processing to digitalization of their processes have significantly increased the efficiency of businesses. Data collected and stored in digital form can now be processed and manipulated to make intelligent and well-informed business decisions. As companies and government institutions continue their digital transformation drive, this leaves a huge volume of customer data in their custody and a considerable exposure to data risk (McKinsey & Company n.d, 2020). Considering the indefinitely susceptible cyber attacks within the digital space and exposure of sensitive data, user data protection and privacy has become an important area of discussion for data handlers (Guo et al., 2021). Organisations are now more than ever under the increasing compulsion from regulatory bodies within their operating domain and the customers they service in ensuring that customer data entrusted to them are responsibly used and adequately protected.

The need to avoid sanctions of regulatory agencies and build a strong consumer trust now necessitates collectors and disseminators of data to develop a data program that provides a clear and honest information on what data is collected from consumers and how they are being collected and stored, indicate how data collected are used, and ultimately provide assurance that data are processed appropriately. To develop an effective data program, a guideline that provides governance for the program is necessary and this introduces the concept of Data Ethics.

According to Harvard Business school business insight, data ethics is the moral obligations of gathering, protecting and using personally identifiable information and how it affects individuals (Harvard Business Insight, 2021). Organisations that collect, store, and use data are constantly faced with ethical questions bothering on data ownership, transparency, consent, privacy, compliance, and intention (IT Business Edge, 2022). Data ethics is all about doing the right thing with data and businesses must continuously make decisions about not only what is legal but also what is behaviourally right in order to prevent data mishandling and improve customer confidence in business processes (Collibra, n.d, 2022).

Businesses processes these days are heavily software driven and software development teams are often faced with the challenge to develop applications that are robust, reliable, and capable of meeting customer deadlines and budget. While the recent introduction of DevOps practice into software development aim to close the communication and collaboration gap that often exist between the development team and the operations team and also hasten development of new product and easy maintenance of existing ones, the socio-technical nature of software engineering practice which involves interaction between people and technology and also the continuous rise in ethical standards within the business world (Majluf & Navarrete, 2011) makes data ethical concerns a major factor that should be prioritized in the DevOps.

Process automation is one of the fundamentals of DevOps and the possibility of over reliance on tools at the expense of organizational structure which may eventually weathered down the oversight function of organizations on data ethics in business operations (Floridi & Taddeo, 2016) is a likelihood which companies can not afford to disregard. In DevOps the zeal to optimize release frequency and velocity may sometimes come at a cost and one of such compromise is on regulatory compliance especially when unscrupulous and uninformed programmers are involved (Abrahams & Langerman, 2018; Skenderi et al., 2020). The global nature of software business and the need for frequent software releases in DevOps also introduces the need to keep the DevOps team constantly in-tune with Data Ethics best practices for different clients in the global marketplace.

1.2 Scope of the thesis

The scope of this thesis is limited to ethics related to the usage of client data entrusted to the care of the DevOps team. More emphasis will be on the use of personal data and the basis of ethical consideration will be drawn mostly from major countries who have fully established guidelines and regulations for ethical usage of personal data. Ethical discussions within this thesis does not cover other areas of ethics or morals expected within software development or IT operations.

1.3 Goal, methods and expected outcome of the research activities.

This thesis intends to research and find out how programmers and operations team within the DevOps practice embrace the concept of Data Ethics. The report will investigate the level of awareness of Data Ethics within the DevOps team and how organizations respond to challenges

associated with unethical data usage within the scope of DevOps. Strategies on how data ethics can be further strengthened within DevOps will be proposed and a model will also be created based on the findings of the research to enhance Data Ethical best practices within DevOps.

The developed model will include a clearly defined data ownership structure and escalation process that caters for data ethical breaches, and this will be evaluated to confirm that it significantly improves the Data Ethics practice within DevOps. It is sincerely hoped that the model along side data ethics awareness recommendations will help business units or organisations who adopt DevOps to improve Data ethical practice within their process, reduce the risk of sensitive data exposure, avoid penalties that comes with violating data laws and help them to earn and maintain the trust of their clients.

The research will follow a design science research approach which generate artefacts that will be useful in solving problems identified in the research. The research problems will be identified in the literature review. Data for the research will be collected through selective interviews of identified DevOps professionals based on experience and geographical spread. The received qualitative data will be analysed using thematic analysis method to identify common patterns. The outcome of the analysis will form the basis of the research recommendations and the artifact to be developed. The created artifact will be validated by seeking feedback and expert opinions from specialist in the DevOps industry.

1.4 Research Questions

The following are the research questions that have been formulated to fulfill the purpose of this research.

RQ1. *Are programmers and operations teams aware of data ethical issues and their implications?*

RQ2. *What tools and processes are available to identify data ethical concerns in DevOps?*

RQ3. *What are the effective controls, monitoring, and reporting channel for Data ethical problems within the DevOps team and organisation?*

RQ4. *Who should be responsible and accountable for ethical data practices in the DevOps team and organization?*

2 LITERATURE REVIEW

In this chapter, related studies performed by other researchers in the field of data ethics, privacy and DevOps are introduced and reviewed. DevOps is an organizational practice that targets team unification and process automation, and the available literature resources on DevOps have diverse scopes of study and focal points with limited number of research studies on how data ethics and compliance can be integrated into and evaluated in DevOps practice (Ramaj et al., 2022). However, some papers have been identified to contain information that can contribute significantly to the research.

2.1 Relevant research works on DevOps and Data Ethics

Virmani, M. (2015) in his research presented how DevOps can be better understood and further made attempts to bridge the gap from continuous integration to continuous development. The researcher set out to cover all relevant sections of DevOps related to the phases of Software development life cycle (SDLC) and shows the DevOps approaches with respect to the software delivery pipeline. More emphasis is also made on the continuously changing business environment and why technology must be agile enough and improve on adopting automation to respond quickly and meet the dynamic needs of businesses they support. The paper also provides in-depth information on factors that organizations planning to adopt DevOps must consider before embracing the practice and how organizations adopting DevOps can move seamlessly from continuous integration to continuous delivery alongside how the benefits of DevOps can be maximized.

The researcher informed that some of the benefits organizations adopting DevOps can realize include consistency of deployment due to repeated process, developers being able to perform validation task in environments similar to production because of continuous deployment model and sharing of resources between team which results in significant cost savings since deployment is automated thereby eliminating the need to reserve unused resources. The paper concluded that DevOps only defines the set of principles but the choice of technology and how the technology is adopted towards realizing the DevOps approaches and practice is completely to be decided by individual organizations and teams embracing DevOps.

The need for more consideration for ethics in technology related practice and research is the focus of Johnson & Smith (2021). The researchers opined that there is significant possibility for unanticipated, unacceptable, and dangerous consequences for technology users with the increase in the amount of data used in driving automated decision-making processes especially as related to machine learning technologies integration into Software. Johnson & Smith (2021) created a synopsis of current work in ethical computing with more emphasis on efforts related to data-driven software development. In their work, theoretical research on software ethics bothering on ethical governance, components of ethics and how the gap between theoretical ethics conversations and practice can be closed were concisely explored.

An empirical study on ethics in software engineering was further carried out by the team. The intention of the study is to provide a foundation for improving ethical practices based on factual evidence. Some of the review of the previous research carried on how developers implement or ignore ethics in software development indicate that developers often take responsibility only for issues bothering around software development such as bugs detection during testing while organizational structure or processes to confront ethical related concerns do not exist. In a particular case study, the developers collectively agreed that ethics consideration is important and beneficial to their organization while they also unanimously stated that their organizational practices do not factor in ethics in any of its processes.

With the review of the existing works, the researchers were able to identify ethical related gaps in software development practice and ample suggestions for future work on how these gaps can be closed were provided. The paper concluded that it is crucial to investigate the possibility of developing and integrating tools that can support ethical concerns in the various stages of data-driven software development pipeline. The Author suggested the need to have tool that supports identification of ethical breaches; however, no model was designed to assist in further development of a suitable tool.

The perspective and mindset of coders about ethical issues in DevOps is the focus of Skenderi et al. (2020). In the paper, the researchers examined the point of view of programmers engaged in DevOps practice with the intention of gaining insights into how versed they are about principles in ethical coding, how often they practice these ethical codes of conduct and to investigate if they

are involved in unscrupulous coding practice. The work starts with a prologue of DevOps in Software engineering practice including the concept of enabling the development and operations team to collaborate.

A detailed description of the roles of DevOps engineers in introducing processes, tools, and methodologies to cater for all demands ranging from coding to deployment and maintenance of the application in the SDLC was enumerated. The researchers further took a deep dive into the various DevOps tools that empower organizations to practice DevOps, and they classified them as log monitoring tools, system monitoring tools, network monitoring tools, build & test tools, and deployment & configuration tools. Skenderi et al. suggested that selecting the right set of tools makes DevOps promise of improving speed, efficiency, and reliability feasible.

The researchers informed that the main reason for the need of ethical coding is because of complex regulatory requirements affecting coding processes and data handling for products affecting healthcare and other sensitive sectors. Coding ethics is expected to set forth professional values, ethical principles, and guidelines by which programmers' actions can be evaluated and judged. From the online survey carried out on 40 software developers involved in DevOps to understand the perception of programmers about ethical considerations, the researchers identified that having fun, business benefits and malicious intentions are the main reasons for unethical code.

Skenderi et al. (2020) concluded that even though most developers who participated in the survey have good attitude towards ethical issues, there is a huge information gap on ethics, and this can result in high risk of unethical practice in coding which ultimately will affect the business and society. The researchers proposed that raising awareness at learning institutions, educational training centres and corporate training programmes about unethical codes and their consequences will be an effective way to mitigate against the chances and risk of unethical code practice. Despite the emphasis on raising awareness, no suggestion on a structured data ethics awareness training or how to manage malicious coders was provided.

Floridi & Taddeo (2016) in their Paper titled "What is data ethics" informed that Data ethics as new branch of ethics is not only built on foundations of computer and information ethics but also more aligned towards being data-centric than information-centric. This shift away from information ethics to data ethics provides the opportunity to concentrate more on data which is

being handled. The researchers indicated that the focus of data ethics is on the different moral dimensions of all kinds of data without excluding even the ones that do not eventually generate information.

In the opinion of the researchers, the huge opportunities data science provides in improving public and private life is not bereft of its own challenges as well and key of these challenges bothers around ethics. They pointed out that as more personal and sensitive data is processed using automated technologies, the continuous reduction of human involvement and oversight functions can pose issues on fairness, responsibility, and human right abuses. Floridi & Taddeo (2016) indicate that ethical challenges in data science should be examined from three intertwined perspectives. These are "ethics of data" which focuses on ethical problems arising from collection and analysis of huge datasets and its antecedent trust and transparency issues, "ethics of algorithm" bothering on artificial intelligence and agents which often results in moral responsibilities and accountabilities on the part of designers of these machine learning applications and "ethics of practices" which is targeted at the responsibilities and liabilities of people and organizations entrusted with handling of data and how they manage consent and user privacy.

The researchers emphatically suggest that ''on the one hand, overlooking ethical issues may prompt negative impact and social rejection while on the other hand, overemphasizing the protection of individual rights in the wrong contexts may lead to regulations that are too rigid, and this in turn can cripple the chances to harness the social value of data science". The paper concludes that for ethical challenges to be addressed successfully, there must be a balance between development and application of data science and the respect for the right of users of these applications and that a failure to advance the cause of ethics will have undesirable consequences for both users and data handlers. The authors identified the need for a balance between practice and right of users but didn't provide any framework or control to measure the level of balance.

Exploration of the nature of data, personal data, data ownership, consensual and purposeful use of data, trustworthiness of usage by data handlers as well as matters bothering on data privacy and confidentiality are the focus of Hand (2018). In the paper, the researcher reiterated the need for ethical oversight and constraints on data storage and tools for extracting and processing information from data to prevent their misuse. Hand indicated that it is more difficult to handle

ethical issues involving data because it is present and found everywhere, can be intrinsically complex and they have the potential to influence all aspects of human endeavours. The author informed that while taking ethical matters into consideration, the current and future use of data must be factored in because data environment changes swiftly. The researcher suggests a shift from the current emphasis on risk and protection during ethical consideration to a more appropriate equity between risk and benefits.

A checklist of topics to be considered while ruminating on data ethics was also provided by the researcher. This includes identification of the body to provide oversight for ethics in organizational processes, awareness of institutional policies and procedure, secure data storage, efficient data management plan, data modification records, data retention policies, data access management, data correction and deletion systems, and global regulations & laws. Hands concludes that ethical codes for data will provide guidance for data handlers on how best to behave in difficult situations, enhance data privacy so that users and public will have increased level of trust, guarantee the beneficial use of data for the public, improve the public perception and integrity of organizations who collect and process data, and overall reassures the employees that they are working for a credible organization.

Oh et al. (2021) in their paper indicated that the integration of technologies into health care system has increased the security and privacy issues associated with health data. The researchers identified the major components of modern electronic health systems and then performed a review of security and privacy studies of each of these components. They stated that e-health data remains one of the most confidential information for individuals and that the regulations and privacy protections such as GDPR and HIPAA that were established to improve the healthcare data governance have not been able to sufficiently protect against e-heath data breaches. The paper suggests that for electronic data breaches to be prevented, security and privacy issues must be given adequate attention. Reviewing related studies and surveys, the researchers provided a categorization of security concerns, requirements, and solutions for e-health data.

Figure 1: Classification on security and privacy for e-health data (Oh et al. 2021)

How organisations adopting DevOps practice can handle the challenges that often arises when they attempt to comply with industry standards, framework and best practices without compromising on the velocity or speed of automated delivery and deployment is investigated by Abrahams & Langerman (2018). The authors maintained that complying with standards within automated environment requires a lot of effort and to meet up with technical regulatory compliance without negatively impacting on delivery time and cost estimates, it is essential to embrace compliance at velocity which allows the possibilities to automate regulatory compliance into product and services delivery. The writers are of the strong opinion that compliance at velocity can seamlessly integrate into DevOps environment because of the similarities in principle of both practices.

Four articles focused on DevOps, compliance and Security were analysed to gain insights into how information security compliance can be improved while still maintaining the velocity of delivery and deployment taking into consideration both the compliance of velocity and DevOps principles. Abrahams & Langerman (2018) observed that even though it is possible to embed security into the delivery and deployment pipelines in DevOps, it is impossible to automate non-technical or personnel-based regulatory compliance processes within the DevOps environment. The authors are of the opinion that this makes DevOps methodology a risk to the organisations practicing it should they fail to provide other means of ensuring regulatory compliance for non-technical related processes. Despite the reality and confirmation of risk for non-technical related compliance requirements within the DevOps environment, the researchers did not suggest ways to mitigate

these risk possibilities.

The suitability of DevOps in regulated software development is the focus of Laukkarinen et al. (2017). In the paper, the authors are of the opinion that implementing modern approaches in software development in environments that are regulated introduces significant challenges due to mandatory governance policies and compliance requirements. A correlation of medical devices software development using DevOps approaches was studied by the researchers. The authors observed a conflicting relationship because DevOps is heavily built on continuous integration and deployment while software development in regulated environments requires rigorous audits and approval processes before release. To understand the benefits and obstacles, the researchers considered two related medical devices and health software IEC/ISO standards IEC 62304 and IEC 82304-1 standards.

The findings of Laukkarinen et al. (2017) shows that while DevOps supports and aligns with regulated software requirements in areas concerning software development procedure, deployment repeatability, item identification and post-market reporting, it however introduces significant challenges in areas where there is strict requirement for completion of software unit verification testing in medical standard before any integration testing can commence. This contrasts with DevOps practice of continuous integration. Another area of conflict involves the regulatory requirement for completion of all tasks and activities before software release which negates the practice of continuous deployment in DevOps.

Laukkarinen et al. (2017) concludes that the current DevOps practice and tools are not suitable and robust enough to cater for software development in regulated environments and suggested that new tools and methods should be explicitly created for the use of DevOps in regulated software development. The writers exposed the need to improve on existing DevOps practice to cater for development in regulated industries but did not provide any suggestion on specific areas of improvement or approaches to follow.

Farroha & Farroha, (2014) discusses the need for organisational culture change to be able to manage security, regulatory compliance, and trust in the DevOps environment. The authors are of

the opinion that ensuring compliance becomes more challenging because of the excess workload and pressure on operations team implementing DevOps. They informed that adjusting workloads appropriately reduces the likelihood of team members being overwhelmed. They also highlighted the need to empower stakeholders with resources that will facilitate compliance with regulations on data and its usage.

For the organisation to enforce compliance, there is a need to put in place automated system that monitors, detects, notify, prevent data loss as well as limit the impact of breaches. In the paper, Farroha & Farroha, (2014) strongly emphasised on the need for policy to be put in place in organisations. The researchers proposed a framework that will ensure the performance and security outlook of the organisation is not compromised as DevOps is implemented to enhance the speed of delivering continuously updated services.

2.2 Overview of software development and data governance policy

2.2.1 Change in software development practices

The traditional waterfall software development process is a unidirectional and pre-organized stages of the SDLC which is based on the premise that customers requirements are precise and static. This model is no longer attractive due to its rigid structure, which is in variance with the dynamic and volatile nature of most customer requirements. Adopting this linear sequential phase for software development task often impact negatively on project delivery especially in aspects of effort, cost, time and customer relationship (Team, n.d.). In 2001, the agile manifesto was created, and this has led to a remarkable change in the software engineering field.

These days most modern software development processes have embraced the agile approach to software development. In agile, software organizations move away from static to a more dynamic development process where software development is iterative and driven by customer needs. Developers are expected to deliver working software to clients in regular short intervals. Overall, Agile approach to software development has enabled a flexible development process in an environment where client's requirements usually change alongside new project deliverables (Dingsøyr et al., 2012).

2.2.2 DevOps Challenges and Impact on organizational structure

Despite the gains of agile methodology in making developers and development cycles more efficient and customer centric, the practice did not adequately address the communication and collaboration gap that often exist between the development team and the operations team. The emergence of DevOps around 2007 addressed the collaboration challenges that often arise when developers who write the codes work independently from the operations team who are responsible for deployment and maintenance of the code. This collaboration challenges introduce unsteady delivery of software and difficulty in deployment because of more reliance on manual processes. With adoption of DevOps, collaboration is enhanced and the two teams no longer work separately but are now merged into a single team that works across the entire SDLC (Atlassian, 2018).

Macarthy & Bass (2020) in its paper "An Empirical Taxonomy of DevOps in Practice" describes DevOps as a set of cultural philosophy, practices and tools that makes use of cross functional teams to reliably build, test and release software faster through the adoption of technology automation. The aim of DevOps is to strengthen team self-responsibility, enhance communication and collaboration between the Software Development & IT operations team and to entrench the practice of process automation using technology toolchains. According to Atlassian (2018), the positive impacts, and benefits of DevOps on organizations adopting the practice include releases that are faster and easier, improved quality of product, better team efficiency due to improved collaboration, enhanced security and ultimately happier teams and clients.

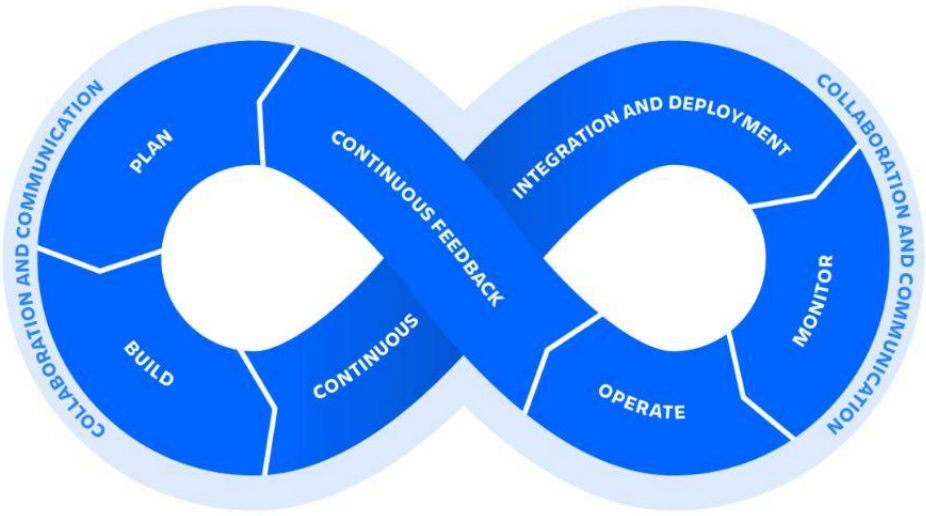

Figure 2: DevOps Life Cycle (Atlassian, 2018)

The embracement of DevOps by organizations also introduces challenges which impact the organizational structure. Most of these challenges are significantly as a result of cultural shift due to new way of working and this is a recurring discussion when technology adoption is discussed (Zhu et al., 2016). One of such numerous concerns this cultural shift introduces is data ethical issues. Data ethics encompasses the code of behavior which determines the morality of what is right and wrong when handling data. According to Floridi & Taddeo (2016), Data ethics is an emerging branch of ethics that is concerned with studying and assessing moral problems related to data including but not limited to its generation, recording, curation, processing, dissemination and use.

2.2.3 Global Data Protection Laws

Businesses are subject to regulations in their operating regions. One of the importance of being aware of ethics of data usage is compliance with regulatory policies. The improper handling of customer personal data in the custody of such handlers has necessitated governments and regional organizations globally to establish laws that regulate the collection, storage, usage, dissemination, and disposal of customer data. These laws and guidelines provide a basis for proper handling of personal data and enforcing data ethics rules. Another importance of data ethics to organizations includes the need for businesses to prove that their processes are trustworthy, develop a good public outlook and adhere to fair and reasonable data usage (Michelle, 2021). The data protection laws of some selected countries are listed below.

Table 1. Data protection Laws in some countries (*DLA Piper Global Data Protection Laws*, n.d.)

Country	Law	Data Security Features
EU	General Data Protection Regulation (GDPR)	GDPR defines personal data as any data that is related to, identifies, describes, or could be associated with a person (or "data subject" as people are referred to in the legislation. The law expects organizations to have some data security precautions in place but is not specific

		about what those precautions must be exactly. GDPR also limits the transfer of personal data out of the European Economic Area (EAA)
UK	Data Protection Act (DPA)	This is the UK's implementation of the GDPR. Everyone responsible for using personal data must follow the strict rules called data protection principles. Also, customers have the right to be informed about how their data is being used and have their data erased.
USA	Health Insurance Portability and Accountability Act (HIPAA)	The Law stipulates that personal information maintained by healthcare bodies must be protected from theft and fraud. It prohibits healthcare providers and businesses from disclosing patient information to anyone other than the patient or their authorized representative.
SOUTH AFRICA	Protection of Personal Information Act (POPIA)	Came into operation in July 2020. Covers not only personal data but also companies and other types of organization. Data processors must give customers a reasonable opportunity to object to processing their data if they wish and communications must include details of how to opt out. They also must implement appropriate technical and organizational security measures to protect personal data in their possession
BRAZIL	Lei Geral de Proteção de Dados Pessoais (LGPD)	Similar to the GDPR, the data privacy law entails data security. Data managers are expected to implement appropriate technical and organizational measures that ultimately protect personal data they are entrusted with.

2.3 Research gap and Summary of the Literature review

This chapter has provided an overview of previous works done within the area of research. Table 2 provides a synopsis of the key findings in the literature review. The analytical feature of this literature review has helped to reveal where problems still exist in the research domain and justify the need for further research. This has also influenced the construction of the research and interview questions (See chapter 4). From the literature review, it can be deduced that the need for data ethical consideration in DevOps practice remains paramount (Floridi & Taddeo, 2016). Some of the authors have emphasized the need to strengthen awareness and trainings so that developers and operations teams can be abreast of data ethical challenges and benefits.

Despite these revelations of lack of awareness as a primary reason for data ethical breaches, there are no studies proposing a structured approach towards bridging this awareness & training gap in the reviewed literature (see Skenderi et al., 2020; Floridi & Taddeo, 2016). Also, none of the research works proposed a conceptual model that provides a holistic approach towards data ethics within the DevOps practice. There are also no studies in the literature indicating the appropriate organisational structure and escalation/response strategy as well as available industry software tools that can be integrated into DevOps to mitigate the risk of data ethical challenges (Abrahams & Langerman, 2018; Farroha & Farroha, 2014; Laukkarinen et al., 2017).

In this thesis work, research will be conducted on how organizations practicing DevOps currently handle data ethics including the identification, assessment, reporting, monitoring, and control processes available in organizations to mitigate against data ethical breaches. A process model for data ethics implementation in DevOps will be developed and validated while Suggestions on improvement strategies for enhancing data ethics in organisations adopting DevOps will also be provided.

Data triangulation of the identified factors responsible for non-compliance to data ethics from the literature review will be performed against the results of the data analysis obtained from the research interview. This will further strengthen the validity and reliability of the research findings through corroboration. The outcome of this research will contribute to the existing body of literature. The research methodologies used for the purpose of this research will be elaborated on in a subsequent chapter of this thesis.

Table 2. Overview of reviewed literature

	Author	Title	Purpose	Key Findings
1	Virmani, M. (2015)	Understanding DevOps & bridging the gap from continuous integration to continuous delivery	To comprehend DevOps, its business benefits, and factors to consider before its adoption.	DevOps need to be applied to the various stages of the SDLC and not limited to development and operations handoff. Organisations are at the liberty of deciding how and what type of technology to adopt in DevOps implementation since DevOps is only a set of principle/practice. Time & cost saving, organisation efficiency and continuous feedback are some of the most significant benefits.
2	Johnson & Smith (2021)	Towards Ethical Data-Driven Software: Filling the Gaps in Ethics Research & Practice	To identify ethical gaps in software development practice and suggest how future works can help resolve the challenges.	Coders are more concerned with fixing bugs and less focused on ethics. Also, processes to tackle ethical concerns are often not in place in organisations. Integrating automated tools that can address ethical breaches in software development pipelines can help improve ethics.
3	Skenderi et al. (2020)	Ethics in DevOps, The attitude of programmers towards it	To obtain opinion of coders on ethics in software development and provide reasons for ethical breaches	Fun, business benefits and malicious intentions are the main reasons for unethical code. There exists a huge information gap on ethics amongst developers and this has heightened data ethical risk. Increasing awareness about unethical codes and their consequences is an effective approach towards mitigating the risk of unethical code practice.
4	Floridi & Taddeo (2016)	What is data ethics?	To provide an overview of ethics as it relates to	Lack of human oversight in automated systems can result in abuse of personal and sensitive data. There should exist a

			data usage in digital technologies	balance between application development and the respect for the right of users of the applications. Failure to promote data ethics will cause unpleasant repercussion for both users and data handlers.
5	Hand (2018)	Aspects of Data Ethics in a Changing World: Where are we now?	To explore the key principles of data ethics and provide checklist of topics to consider in data ethics	There is need for constraint and oversight when using tools to process personal data. Data environment is dynamic, hence the need to consider current and future use of data. Data ethics should be viewed from the risk and benefit perspective rather than the often risk and protection approach.
6	Oh et al. (2021)	A Comprehensive Survey of Security and Privacy for Electronic Health Data	To investigate and suggest solutions to the factors responsible for security and privacy concerns in electronic health systems	Existing regulations and privacy protections such as GDPR and HIPAA do not sufficiently protect against e-heath data breaches. Access restriction, data confidentiality, data integrity, data availability, data anonymity, auditability and accountability are some of the requirements to consider when strengthening data security and privacy.
7	Abrahams & Langerman (2018)	Compliance at Velocity within a DevOps Environment	To investigate and suggest solutions to regulatory compliance challenges in DevOps	Compliance at velocity allows the possibilities to automate regulatory compliance into product and services delivery without affecting the speed of automated delivery and deployment. It is impossible to automate non-technical or personnel-based regulatory compliance processes within the DevOps environment and this makes DevOps methodology

				a risk to the organizations practicing it if they do not adopt other method of ensuring compliance.
8	Laukkarinen et al. (2017)	DevOps in Regulated Software Development: Case Medical Devices.	To investigate the suitability of DevOps in regulated software development such as medical applications	There are conflicts in medical device software lifecycle requirement standards and DevOps because of the need for thorough audit and approval processes in these standards as against continuous integration and deployment principle in DevOps. Existing DevOps practice and tools are not suitable and robust enough to cater for software development in regulated environments.
9	Farroha & Farroha, (2014)	A Framework for Managing Mission Needs, Compliance and Trust in the DevOps Environment	To provide a framework that ensures performance and security compliance is not jeopardized because of increased speed of deployment in DevOps	Compliance to regulatory and business standards is more challenging due to the excess workload and pressure on team implementing DevOps. Policy implementation, integration of automated compliance systems and providing stakeholders with resources that will facilitate compliance with regulations on data and its usage can mitigate breaches and strengthen compliance in DevOps.

3 RESEARCH METHOD

As discussed earlier, the overall goal of this research is to find out how data ethics is considered and handled by organisations implementing DevOps, the level of awareness by the development and operations team, the challenges faced in implementing data ethics and finally the strategies that can be implemented to address the identified challenges and enhance data ethical practices within DevOps. This chapter provides an overview of the research methodology used in carrying out this research.

As mentioned briefly in the introduction chapter, this research is conducted using Design science research methodology (DSRM). Design science provides a procedure for the evolution of new ways to enhance human organisations, especially as it relates to and affects social aspects, through the activities of designing, developing, demonstrating, evaluating, communication and modification of technological artifacts (Baskerville et al., 2009). When DSRM is used in research, its main purpose is to create artifacts that can solve identified problems (Vaishnavi & Kuechler, 2015). The artifact in this thesis will be a conceptual model that provides solution to identified data ethical challenges and eventually enhances the adoption of Data ethical practices in organisations that embrace DevOps. The procedure for conducting design science research, the technique used to collect data in the study and the approach used to analyse the data collected are all discussed in the below sections.

3.1 Design Science Research Method

There are two remarkable features of DSRM. The first being that the outcome of the research will direct or prescribe to users of the solution on what to do rather than just providing suggestions and the second feature is that it is necessitated by the desire to solve human challenges. The outcome of DSRM are artifacts which can comes in the form of constructs derived from ideas that are subjective and not founded on experimental evidence, models which are conceptual representation of a proposed system, methods which are established procedures for approaching a problem or instantiations of existing artifacts (Hevner et al., 2004).

In deciding on choice of research methodology, Venable et al. (2017) explained that one significant difference between social or natural science and design science (DS) is that DS has a considerable

reliance on functional explanations that are deeply rooted in the relationship between functional requirements and prescriptive components of the designed artifacts. March & Smith (1995) also opined that while social and behavioural sciences attempt to comprehend and seek insight into reality, the main purpose of Design Science Research is to innovate new means for performing in the world in order to modify or advance reality.

3.1.1 Rule of practice for Design Science Research (DSR)

Practice rules are statements that are generally applicable and affect matters relating to procedure or practice in a discipline and its purpose is to regulate the methods used to conduct business in that particular domain. Hevner et al. (2004) maintained that the most important attributes of a properly carried out design science research are:

- The research process must generate a viable artifact that will address a problem.
- The produced artifact must be relevant in solving a critical business problem that have previously not been resolved.
- The artifact must show evidence of rigor in both its construction and evaluation. The artifact's claims of quality, usefulness and effectiveness must be meticulously assessed.
- The design science research that produced the artifact must follow a search process and should build on previous research work and existing theories or knowledge.
- The outcome of the research must be adequately communicated to the relevant audience.

3.1.2 Guidelines for conducting DSR.

Van der Merwe et al. (2020) provides six (6) useful guidelines for conducting design science research in information systems. This guideline is expected to provide researchers embarking on DSR with information suggesting how it is to be carried out. The guidelines are:

1. The researcher should contextualise DSR and determine its appropriateness in the field of Information systems and be able to differentiate various concepts such as design, design science and DSR.
2. Understand the fundamental knowledge or philosophy that serves as basis for the research and the discussion on the nature of DSR.
3. Acquire information on the historical viewpoint of DSR and examine the work of the trailblazers in the field.

4. Appraise the role of the artefact in DSR and the various views on design theory. Design theory attempts to explain why a design is done in a particular way and how things put together influences or directs the audience and hence make the design work.
5. Select a suitable option from the various available DSR process model for implementation of the research study.
6. Formulate how research outcome obtained from the DSR would be communicated in the report.

3.1.3 Steps in conducting DSR.

When undertaking a design science project, two main components are involved. The first being the object of study which is the artifact and the second is the activities involved which includes designing and investigating the artifact. The design activity requires the researcher to know the goals of the project and the social conditions of the stakeholders of the research project while the investigative activity requires the researcher to be acquainted with knowledge context of the project (Wieringa, 2014).

Peffers et al. (2007) synthesized seven research papers on DSRM process models and develop a process model that consist of six (6) activities in a nominal sequence that a researcher should follow when performing design science research. The common design process elements are:

Step 1: ***Problem Identification and Motivation***. At this stage, the specific research problem is defined. The definition of the problem will be useful in developing an artifact that provides a solution to the problem. This stage also requires justifying the value of the solution in order to motivate the researcher and the targeted audience in finding a solution and accepting the result of the research.

Step 2: ***Define the Objectives for a solution***. Here, knowledge of the situation of the problem and currently available solutions and their effectiveness is required. The researcher at this stage also provides explanation to how the new artifact that will be designed will support and provide solution to the problem that has not resolved.

Step 3: ***Design & Development.*** This stage involves the construction of the artifact. The artifact's expected functionality and architectural are first conceptualized and thereafter the actual artifact is developed.

Step 4: ***Demonstration***. The stage involves exhibiting that the artifact solves the problem.

Step 5: ***Evaluation***. At this stage, the earlier defined objective of the solution is compared with the actual observed results obtained at the demonstration stage. The intention is to determine to what extent the artifact can provide solution to the problem.

Step 6: ***Communication***. This stage involves communicating the outcome of the research, the importance of the research, the efficacy of the solution, the thoroughness of the design process and any other important activities to appropriate audience such as researchers and professionals.

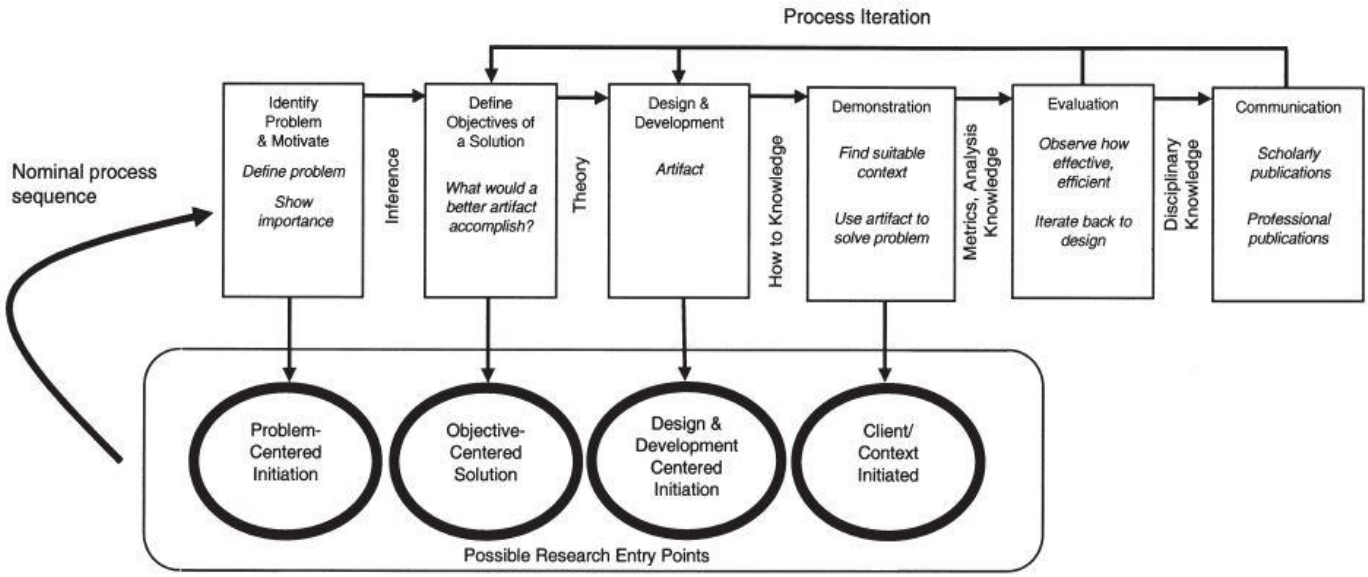

Figure 3: DSRM Process Model (Peffers et al. (2007))

3.2 General Literature Review

Literature review is an economical and time-saving approach for gathering evidence about a research topic. The literature review for this thesis study followed a non-systematic approach. The review does not follow any defined formal methodology and there is no quantitative analysis of the findings obtained from the review. This process entails a well-informed selection of more recent and high-quality articles and papers on the research topic. The reason for selecting this approach is to be able to recognise and connect trends in the research domain in order to have a clearer understanding of the research. Also, it produces moderate size document, and the output of the literature review is usually easy to understand since it requires less technical skills to produce (Director et al., 2015). All these reasons make non-systematic literature review a more suitable approach in this research since the review is just for information finding purpose and there is no formal reporting requirement for the literature that may necessitate an all-encompassing review.

The literature for the non-systematic review (NSR) was searched for and obtained primarily from google, google scholar and IEEE Xplore digital library using the following search strings:

- Data ethics
- Data ethical challenges
- DevOps Practice
- Development AND operations AND ethics AND Data Ethics
- Implications of Data Ethics

The purpose of the search process is to identify and pick out papers in which DevOps, Ethics and Data Ethics are mentioned. Keywords used for the search were selected by breaking down the research questions. The search for relevant papers also involved cross-referencing the reference list of already identified suitable papers. The search was limited to only recent papers published between 2012 and 2022. Consideration was for conference papers and journal articles where factors related to Data ethics and/or DevOps are discussed while Blogs and PowerPoint presentations have been excluded. At the end of the meticulous search and selection process, thirteen (13) papers were selected as suitable for review after carefully examining the title, perusing the abstract and eventually reading the entire content.

3.3 Data Analysis Method

3.3.1 Qualitative Data Analysis

The data analysis method employed in research is important for the credibility of the work performed. The data collected from the interview process in this study is qualitative in nature. Qualitative data is usually descriptive, non-numerical, and conceptual, reflecting individual's experience, perception or opinion (UKData Service, 2020). Investigating and gaining insights into qualitative data requires qualitative data analysis approach. The process assists researchers to illustrate, classify and interconnect events within the research concept (Graue, 2015). Qualitative analysis consists of three different activity flows that happen simultaneously (Miles & Huberman, 1994). These are:

- **Data Reduction** where transcribed data is abstracted and simplified.
- **Data Display** where various data visualization techniques such as figures, tables, graphs,

and descriptive text are used by the researcher to produce proof, buttress, and substantiate interpretations.

- **Conclusion drawing/Verification** which is the last stage where the research ideas and reflections are grouped and presented logically.

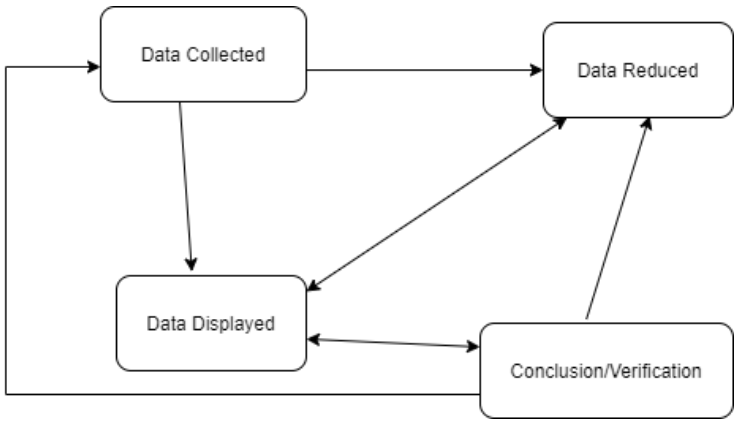

Figure 4: Qualitative Analysis Model (Miles & Huberman, 1994)

3.3.2 Thematic Analysis

In order to organize, analyse and interprete the collected data and ultimately gain useful insights from the interviews conducted, a qualitative data analysis method known as thematic analysis is selected and used in this research. The purpose of thematic analysis (TA) is to show patterns or themes that correlate with the data. Theme expresses or highlights essential things about the research data set and their relationship to the defined research questions. The use of Thematic analysis method to analyse the elicited viewpoints of interviewees gives the researcher the opportunity to have an in depth understanding of the issue being analysed (Marks & Yardley, 2004).

Thematic analysis unlike many other qualitative data analysis methodologies is flexible and not fixed to any specific epistemological or theoretical approach (Maguire & Delahunt, 2017; Braun & Clarke, 2006). Its relative ease of use, ability to adapt to different use cases and capability to provide comprehensive insight into data makes thematic analysis a highly beneficial approach for data analysis. Rather than just counting phrases and words for meaning, thematic analysis allows researcher to have a better grasp of data analysis by recognizing and detailing the implicit and explicit views in the research data (Namey et al., 2008). Thematic analysis is suitable when there

is a need for the researcher to (Alhojailan, 2012):

- **Interprete data**: With the use of thematic analysis, researcher can extract clarifications that are coherent with the data collected in the research. This is made possible as TA is able recognise factors influencing points raised by participants that generated the data.
- **Conduct deductive and inductive analysis approaches**: The flexibility of TA allows it to be usable when there is a need to explore and test the validity of an already known theory or create a theory from studying collected data sets.
- **Analyse data collected at separate phases of research**: Sometimes researchers are interested in observing changes occurring before and after data is adapted. An example is collecting users' opinion about a prospective application before and after it is developed. The use of TA allows researchers to spot the similarities and differences between the pre and post data phases.
- **Code and categorise data**: These are the core activities in thematic analysis. Obtained research data can be coded and categorised into themes representing specific perceptions of the participants that the researcher considers applicable to the research questions.

3.3.2.1 Steps in conducting Thematic Analysis

When conducting thematic analysis, two main components are identified. The "codes" which are primarily detailed highlights of specific and relevant sections of the transcribed text and the other being the "themes" which are condensed representation of codes after patterns have been identified in the codes. Several approaches are available for conducting thematic analysis. However, the most popular representation follows the six-step procedure developed by Virginia Braun and Victoria Clarke, which if carried out thoroughly, has the ability to help avert confirmation bias in qualitative data analysis (Caulfield, 2019). The step-by-step guide proposed for thematic analysis are (Braun & Clarke, 2006):

Step 1: **Familiarization with data**. The aim of this step is to be know the data. At this stage the researcher transcribes the data to be analysed, read through the data to get acquainted with the content, takes down notes and elicit ideas.

Step 2. **Generating initial codes**. At this stage, relevant phrases and sentences are highlighted, collated, and coded into shorter labels. A glance at the code gives the researcher a concise and brief run-through of the salient and repeated points in the data.

Step 3: **Searching for themes**. Themes are derived from codes. They are combinations of several codes with common patterns into single element. In this step, the researcher searches and identify these similar patterns among the previously generated codes and convert the codes into themes. Also, at this stage some codes are revealed to be ambiguous and irrelevant in the data analysis process and are therefore dispensed with.

Step 4: **Reviewing themes**. At this stage, the purpose is to confirm that the themes derived are useful and truly represent the data. The data set is compared against the themes to detect anomalies and avail possibilities of improvement. Such improvement needs can lead to previously defined themes being split, combined, discarded or creation of an entirely new one.

Step 5: **Defining and naming themes**. In this step, a concise and clearly defined name for each theme is created. This makes the data and the overall narrative of the data analysis to be more comprehensible.

Step 6: **Writing the report**. This is the final step, and it involves writing or reporting our findings from analysing the data. The analysis is linked back to the research questions and literature.

4 RESEARCH DESIGN

4.1 Data Collection

The purpose of the research design is to create a plan to answer the research questions. The main approach for collecting data in this research is through interview. This data collection method was chosen because of the socio-technical and qualitative nature of the research topic. The Interview approach used is semi-structured. Here, the questions to be asked during the interview are pre-planned and open-ended. The order in which the questions are asked are mostly based on developments experienced during the interview session. This flexibility in semi-structured interview allows new ideas that can be useful for the research to be elicited (Magaldi & Berler, 2020) unlike structured interview that are generally close-ended and do follow a set order.

4.2 Selecting and Reviewing Interview Questions

The Questions for the semi-structured interview have been developed following the principles of specification, division and tacit assumption (Lazarsfeld, 1935). The questions have been designed to be focused on specific domain of the research study. Applying the principle of division, the questions are constructed so that they are clear enough without ambiguity, each interview question addresses only one section of the research objectives and the sequence follows logical order from less complex to more sensitive questions (Leech, 2002). With the principle of tacit assumption, the questions have been formulated in such a manner that probes the participant to provide responses that are comprehensive enough, eliminating the fear that his responses would be misunderstood and further strengthening trust in the interview session.

Further assessment of the drafted interview questions was carried based on McIntosh & Morse, (2015) guideline to ensure that:

- All necessary questions have been included.
- The questions can elicit the required response from the participant.
- The language of communication is clear and unambiguous to the participant.
- The questions are logically sequenced.
- The Interview guide inspire the respondent to participate in the research.

At the end of subjecting the initial drafted interview questions to the rigors of the above interview guidelines, the following interview questions have been prepared to adequately answer the research questions:

RQ1. ***Are programmers and operations teams aware of data ethical issues and their implications?***

Literature review suggest that programmers are aware of data ethics. However, it is important to find out if team members in the DevOps know about the components that make up data ethics and be sure they understand how it helps drive the success of business. It is expected that the responses elicited will help address knowledge gap and any defective training methods adopted in organisations. The following interview questions provide answers to the RQ1.

- What is DevOps and to what extent is it being practiced in the organisation you work with?
- Does your organisation develop solutions for diverse clients across the globe or is it limited to a specific geographical location?
- What does data ethics mean to you?
- What are the business benefits of adherence to ethics of data usage and implications of data ethical breaches?
- What are the obstacles to achieving high level of data ethics within the DevOps practice?
- Have you found yourself in situations where you needed to compromise on data ethics while attempting to optimize release frequency and velocity?
- Are there formal data ethics awareness trainings in your organisation for DevOps team and how frequently is it conducted?

RQ2. ***What tools and processes are available to identify data ethical concerns in DevOps?***

There are various industry automated tools integrated into software delivery/deployment pipelines. The intention of this research question is to identify automated tools and processes that help address data ethical breaches and non-compliance to regulatory standards. From the literature review, it is recommended that integration of tools into organisational processes will help address non-compliance challenges. However, there are no mention of available industry tools and the types that can address non-technical or personnel-based compliance requirement. The following questions are presented to the interview participants.

- What are the tools in your organisational software toolchain that can assist the DevOps team to identify and prevent data ethical issues?
- How does your organisation ensure compliance to Data ethical and privacy laws and regulations for multiple global projects?
- Is there a data ethics policy and data governance framework in place in your organisation and are you aware of the content of the policy and the framework?

RQ3. ***What are the effective controls, monitoring, and reporting channel for Data ethical problems within the DevOps team and organisation?***

The outcomes of the literature review suggest that there are weak controls for Data ethics and privacy in the DevOps environment. To understand why this is the case and provide effective solutions that can enhance control selection and implementation, the RQ3 has been formulated and the following interview questions are presented to the respondents.

- What are the data ethics control and reporting processes in place in your organisation to mitigate against data ethical issues within the DevOps practice?
- How does your organisation measure and monitor the effectiveness of the controls?
- What strategies do you know that can assist in improving Data ethics within DevOps?

RQ4. ***Who should be responsible and accountable for ethical data practices in the DevOps team and organization?***

Oversight remains important when people and processes are expected to comply. The literature suggests lack of oversight functions as one of the reasons for non-compliance to data ethics in DevOps environment. The RQ4 is expected to identify existing anomalies in the organisation's role delegations pertaining to data ethics so that a more suitable one can be suggested. The following interview questions addresses the RQ4.

- Who is primarily responsible for Data Ethics and Privacy in your organisation?
- Does your organisation and DevOps team have a staff role dedicated to and accountable for Data Ethics?

4.3 Selecting Interview Participants

Six interviewees were selected from development and operations team working in diverse industry such as software and consulting that have embraced and implemented DevOps. The same

interview questions were asked all the participants to ensure uniformity of response as well as obtain a diverse viewpoint on the research. A scaled-down checklist of areas of discussion was shared with the interviewees prior to the interview to make them better prepared. The participants are carefully selected to represent different geographical locations across Europe, North America and Africa since culture and living style have significant effect on ethics. The Interviews were conducted using Microsoft teams call and in-person. The interviewees participation was voluntary, and the identity of the participants are confidential. The interview sessions are recorded and transcribed into text, and each session is an average of forty-five minutes. The transcript has been shared with respective participants to confirm that all details discussed are correctly captured. In table 3, the profile of the participants and industry they work for are presented.

Table 3. Participants profile

Job Designation	Company Specification	Location	Years of Experience
Web Developer	Software-as-a-Service company	Finland (Europe)	5 years in DevOps
Senior Backend Engineer	Software Product development company	Nigeria (Africa)	7 years in software development. 4 years in DevOps
IT infrastructure Administrator	Royalty and copyright Management company	Canada (North America)	8 years in IT Infrastructure Administration & Support. 3 years Implementing DevOps
DevOps Engineer	Consulting firm	Germany (Europe)	2 years Implementing DevOps
Senior DevOps Engineer	Consulting Firm	Germany (Europe) majorly supporting clients in United Kingdom	6 years in IT Infrastructure management 5 years Implementing DevOps
DevOps Engineer	Industrial IoT software company	Germany (Europe)	7 years in IT systems support 2 years in Project Management 3 years Implementing DevOps

The responses of the interviewees are provided in table 6 to 11 in the appendix. However, a detailed analysis of the responses received is performed and presented in Chapter 5 of this thesis.

5 RESULTS

In this chapter, a comprehensive exploration of the results derived from the mapping of the literature review and thematic analysis of interview data is performed and presented. The aim of this activity is to systematically evaluate the obtained data in relation to the research objectives.

5.1 Analysis of mapped literature review

Based on search for articles relevant to the research topic majorly from google scholar and IEEE Xplore digital library, nine (9) papers have provided strong link between ethics, data ethics, software engineering and DevOps practice. From the selected articles, eight (8) factors that can influence and impact data ethics within DevOps practice have been identified and highlighted. The outcome of the mapping of these factors to their respective articles is provided below in Table 4. In this result, the description of these factors and the impact on Data ethics is briefly explained.

Table 4. Mapping of factors identified in Literature.

ID No	Factor	explanation	Relevant Paper
1	Organisational Culture	This is the aggregation of the principles, ethics, morals, expectations, traditions, and other traits that drives the decisions and actions of team members and the organisation at large. Great culture improves ethical performance, and a flawed organisational culture is an hinderance to good ethical practice. The same applies to Data Ethics within the DevOps practice.	• Johnson & Smith (2020) • Hand (2018) • Zhu et al (2016) • Farroha & Farroha, (2014)
2	Lack of Suitable data governance framework	Data governance framework creates a holistic set of rules, processes, responsibility delegation and accountability on matters bothering on collection, storage, and use of data to assure privacy and compliance.	• Johnson & Smith (2020) • Hand (2018) • Floridi & Taddeo (2016)

		Organisations embracing DevOps practice without a suitable data governance framework are susceptible to data ethical breaches and conflicts with regulatory bodies.	• Farroha & Farroha, (2014)
3	Lack of automated tools to support data ethics and regulatory compliance	The essence of automated tools is to speed up and increase the efficiency of managing task that traditionally can be time-consuming and overwhelming. There are several data protection and compliance laws that DevOps must take into consideration before and when processing data. Lack of an automated tool to enhance this decision-making process increases the likelihood and risk of exposure to Data ethical breaches and non-compliance	• Laukkarinen et al (2017) • Johnson & Smith (2020) • Abrahams & Langerman 2018 • Farroha & Farroha, (2014)
4	Data ethics knowledge gap	Knowledge gap is the difference between what an individual knows and what he is expected to know. When this is applied to Data ethics in DevOps, it means the affected team member is lacking in or fall short of the requisite knowledge to identify and comply to expected data ethical standard within the practice.	• Skenderi et al (2020) • Hand (2018)
5	DevOps team member with malicious intention	A DevOps team member with a malicious state of mind in contrast to the Data ethical values of the organisation remains a threat. There is a need to onboard team members with values that are in tandem to that of the organisation to avoid data ethical breaches.	• Skenderi et al (2020)

6	Work strain due to excess workload	DevOps team members are susceptible to work burnout when exposed to psychological stress and hardship due to high work demands. This can result in negligence to regulatory standards, compliance, and laws.	• Farroha & Farroha, (2014)
7	Lack of Data Ethics awareness and training program	The essence of awareness and trainings is to bridge knowledge gaps and sensitize affected parties. Data Ethics awareness and training program is a key controlling factor to mitigate data ethical breaches. When DevOps members are unaware and lack the necessary data ethics training, chances of breaches remain high.	• Skenderi et al (2020) • Floridi & Taddeo (2016)
8	Conflicts between DevOps practice and compliance regulations	Current DevOps practice is incompatible with some compliance regulations especially within regulated industries. These differences in principles and practice expectations can significantly introduce data ethical issues especially when practitioners of DevOps are at a loss on what is right or wrong. Also, complex regulatory requirements and cases where data protection laws are open ended and vague with no clearly defined implementation strategies often results in inadequate protection against data ethical breaches.	• Laukkarinen et al (2017) • Oh et al (2021) • Skenderi et al (2020)

5.2 Thematic Data Analysis of Interview

The six participants responses obtained from the semi-structured interview have been presented in table 6 to 11 in the appendix. These interviewee responses are analysed and presented in this section based on the thematic data analysis approach discussed in section 3.4.2 of chapter 3. The transcribed Interview data have been read through to be familiar with the content, important phrases and sentences have been grouped into codes. The codes are inspected for pattern identification and codes with similar patterns are finally grouped into theme with clearly defined name. The theme further undergoes several reviews to ascertain that the selected theme name is a true representation of the analysed interview data. The outcome of the thematic analysis process including the codes and derived themes are shown in table 5.

Inadequate Awareness and Training on Data ethics has been identified as one of the main factors responsible for data ethical breaches in DevOps practice. Participants 1, 4, and 5 are of the strong opinion that majority of the breaches are because of lack of structured training and awareness for the DevOps team. While participants 1, 2 and 4 confirmed that there are trainings and awareness in place in their organisations for Data ethics, participants 3, 5 and 6 informed that the trainings available in their organisation is focused only on security. Participant 4 informed that due to insufficient work time, most staff just focus on passing the compulsory assessment provided at end of training rather than understanding the content.

All participants confirmed that there are no Data ethics awareness training specifically tailored and prepared for the DevOps team and they only participate in the general training organised for every member of staff in the organisation. The trainings contents are also delivered to the participants as either online or self-study reading, and no provision is made for live in-person training. All participants collectively agree that putting in place a comprehensive data ethics awareness and training program is an effect measure towards addressing data ethical challenges in DevOps practice.

Table 5. Themes and Codes obtained from the Interviewee responses.

	Theme	Code	Description of Code	Sample Interview Extract
1	Inadequate Data Ethics Awareness & Training program	Not properly trained or aware of data ethics	Most organisations trainings for the DevOps team are focused on security and less of on data ethics.	"The trainings are more about security awareness. DevOps personnel do not know what to do when there are breaches" [P1]. "The DevOps person may not have been trained properly on how to handle personal data" [P4].
		Training not specific to DevOps team	The trainings and awareness programs are usually company wide and not focused for the DevOps team	"Sometimes DevOps staff just keep trying to answer the questions several times just to pass the compulsory assessment and not really with mindset to know the training content." [P4]
		Lack of proper education	No provisions made for educating the DevOps team on data ethics	"I think primarily is the lack of proper education, I mean training and awareness among members of the DevOps team." [P5]
2	Data ethics knowledge gap	May not know that they are doing something wrong	DevOps team members may not be well informed on what is right or wrong.	"They may be unaware that they are doing something wrong. They may not know that it is unethical to manipulate a client's data without consent or approval." [P3] "Some DevOps team members might not even know that what they are doing is unethical and constitute data breach." [P5]
3	Excessive work pressure resulting in Negligence	Much pressure on DevOps engineers for quick delivery	Excessive job demand resulting in burnout	"Sometimes the Developers put so much pressure in DevOps engineers and this can lead to data ethical breaches." [P1] "The pressure to get this done quickly may make the developer or the operations person not to follow laid down procedure." [P4]

				"That is because they were under pressure to get the application running as soon as possible and pressure is not just even on the DevOps team only. It can also be on the actual owner of the data which are the clients [P2]
		Data ethics ignored due to DevOps speed	neglecting the expected ethical data obligations	"Data ethics could be ignored or omitted during the DevOps cycle especially when DevOps cycle is running fast." [P6]
		Team carelessness	Failure to give sufficient attention required for data ethics thereby causing negligence	"Carelessness on the part of the team which is human factor, because the actual process or guidelines of DevOps if properly followed will avoid such occurrence." [P5] "The data may be left in a careless way such that unauthorised persons may have access to such information and use it without consent or approval of the client." [P3]
4	Organisational culture	Stronger Advocacy for Security and not Ethics in DevOps	Emphasis is more on securing the system and lesser focus on data ethics	"In DevOps we preach more about Security and hardly on ethics." [P1] "As Developers we do not usually think much about data ethics. We care more about security and getting the code to work." [P6]
		Organisation focused more on security	Organisational efforts are geared more towards ensuring a secured working environment and less discussion on data ethics	"The talks and focus on in my company are more on security." [P3]

5	Lack of Suitable data governance framework	No clear framework and control	Missing structures that can sufficiently guide and support the implementation and maintenance of process	"I think there is no clear framework or control to ensure that privacy is taken into consideration." [P6]
		Data ethics not clearly defined or communicated		"There may be some data ethics consideration, but it is not clearly defined or communicated. I have asked questions on how we do this and that but no clear answer to my questions from those who are supposed to know." [P3] "I am not aware of any data ethics policy or framework in use. I assume all is being handled by the data protection officer, but I am not privy to how it works. For the reporting or communication, I am not clearly aware of it." [P5]
		Weak access control & compliance procedures		"Sometimes team members need help from each other and in the process of requesting or receiving help, other members who ideally have not been setup to have access to specific data may end up knowing what they are not supposed to know." [P4] "Not every industry or company does this practice of senior members of the team dedicated to checking to ensure there are no data compromise before things get into production. In some companies these extra checks are not in place." [P1]
6	Organisational Size	Huge customer base increase concerns for data ethical practice.	likelihood of data ethical breaches increases as clientele grows. This influence organisations decision to be	"The company I worked for before have a huge customer base and they deal with much higher volume of customer personal data. So, they are kind of more concerned about ethical and privacy issues unlike the ones I work with currently." [P5]

		Big organisations have better measures to mitigate data ethical breaches	more ethically aware.	"Most big organizations however have introduced measures to reduce the likelihood of these data ethics occurrence, but this may not be the case with startup companies." [P4] "Most big organisations are scared of fines from regulatory bodies, so they put a lot of processes in place to prevent going against government policies and regulations. The organisation I work for is relatively small." [P3]
7	DevOps team member with malicious intention	Manipulation for malicious reasons	Dishonest behaviour in handling client's personal data in care of DevOps staff	"Customer biodata and financial information stored in a database can be manipulated by backed staff for malicious reasons especially when those data are in plain text and not masked" [P3]
		Mischievous Decision		"The DevOps person may decide to be mischievous despite the trainings on how to handle personal data." [P4]
8	Lack of automated tools to support data ethics and regulatory compliance	Difficult for tools to flag moral obligations	Available automated tools do not comprehensively support adherence to data ethics in DevOps.	"How a software tool can produce such algorithm that can measure, predict, and flag social behaviour is something difficult since ethics is about moral obligations" [P1] "There are no suitable tools to holistically ensure privacy is taken into consideration. I know of only tools that allows clients to delete or handle their personal data remotely." [P6]

knowledge gap on Data ethical best practices is another recognised factor from the conducted interview. Participants 3 and 5 suggest that this insufficient or deficiency in knowledge can significantly introduce data ethical breaches in DevOps as the affected team members carry out activities that are susceptible to data breaches. Participant 3, 4 and 5 understands data ethics from the viewpoint of privacy and consent, Participants 1 and 3 refers to it as data transparency, privacy, and protection while participant 2 believes it encompasses doing the right thing with personal data.

All the participants interviewed showed sufficient knowledge of the concept of data ethics, benefits it offers to organisations practicing it and the implications of non-compliance. Participant 3 informed that even though he has undergone trainings in his previous organisation on GDPR, he is not confident that he completely understands data ethics. However, participants 6 confirms that he does not have the requisite experience in data ethics because he has not undergone any training in such domain in his previous and current company.

Negligence due to Work pressure is another factor responsible for Data ethical breaches and non-compliance in DevOps. All participants interviewed are of the opinion that excessive job demand on the DevOps team raises the likelihood of data ethical breaches, negligence, and non-compliance to data standards. The participants informed that Data ethics is often put in the back burner as work pressure increases. Participant 4 is of the opinion that the pressure can cascade from clients to DevOps team members in an attempt to get the application running as soon as possible. Participant 6 thinks the speed of the DevOps cycle is responsible for the omission while participant 1 blames the Developers for putting too much pressure on DevOps engineers.

Organisation culture which is the disposition of an organisation towards embracing data ethical practices is another key factor affecting data ethics in DevOps practice. Participants 1 and 6 informed that the focus of the DevOps team is more towards Security and less on Data ethics while participant 3 mentioned that the organisation he works for are more predisposed towards ensuring an environment safe from external security breaches and there are no significant efforts or discussion of Data ethics. Participant 2 specifically mentioned that situation arises where his previous employer expects him to manage client's expectations with less care on data ethical concerns that may arise in his course of duty.

The need for a **suitable data governance framework** is essential in ensuring adherence to Data ethical practices in DevOps. With an appropriate data governance framework in place, an organisation can specify and document the rules, expectations, policies, processes, procedures, controls, roles, responsibilities, accountabilities, ownership, reporting, communication channels and key performance indicators with respect to data handled. From the interview conducted, all interview respondents informed that they are not aware of any data ethics policy document or framework in place in their respective organisations.

Participants 1, 2, 4 and 5 confirmed that there is a dedicated role in the organisation with designation "Data protection officer" for issues bothering on data while participants 3 and 6 do not have any dedicated role in their organisations. All participants confirmed that no similar dedicated role exist within the DevOps team. Participant 1 is of the opinion that a role such as Data ethics champion, similar to security champion that currently exist in his organisation's DevOps team, can be created to further strengthen Data ethics within the team. Participant 5 also suggested that there should be an independent body with the responsibility of overseeing the activities of the Data protection officer to strengthen accountability. Participants 1, 2, and 4 informed that their companies put in place training, rigorous approvals, and limited data access respectively as control measures against data ethical breaches while participants 3, 5 and 6 are unaware of any controls in place in their organisations.

All participants are unaware of any measuring or monitoring processes for the controls while only participant 4 informed that there is a clearly defined communication or reporting channel for identified data ethical breaches. Participant 3 suggest creation of a communication channel where team members can report unethical data practices while participant 2 is of the opinion that for a reporting channel to be effective and usable, the reporting process should be made discreet and confidential to prevent persecution or acrimony within the team.

The **size of an organisation** adopting DevOps is another factor responsible for Data ethics awareness and compliance as deduced from the analysis of the interview. Participants 3, 4 and 5 have mentioned that the bigger the organisation and the clientele base, the more the risk of exposure to data ethical breaches and non-compliance to regulatory requirements. According to participant 3, the fear of paying fines make larger organisations to implement several processes

that can mitigate data ethical breaches. Participant 4 thinks startup companies care less about implementing controls that can reduce instances of data ethical breaches while participant 5 is of the opinion that the product line of the organisation is a strong factor influencing the degree of commitment to ensuring data ethical standards.

The possibility of having a **mischievous DevOps team member** is another factor capable of introducing data ethical issues in the practice. The principles of data ethics are strongly based on moral behaviours. Participant 4 informed that enforcing compliance is a herculean task especially when there is conscious intention by a member of the DevOps team to deviate from laid than rules. Participant 3 strongly opines that the moral obligation of protecting personally identifiable information received from clients is at jeopardy when DevOps team maliciously manipulate such data especially when data confidentiality controls are not implemented.

Participants 1, 3, 4, 5 and 6 have not found themselves in situations where they need to compromise on data ethics. Participant 1 have found himself in a situation that leads to compromise, but he refused to, a decision based on previously sound trainings he had received. Participant 2 have consciously compromised data ethics by manipulating and using client's live data for test purpose without consent while participant 6 buttresses the possibility of being in a situation that can result in compromising on data ethics.

Lack of automated tools to support data ethics and regulatory compliance is also identified as a factor contributing to data ethical issues within the DevOps practice. Participant 1 and 6 strongly believes that lack of an automated tool that can holistically and effectively control, measure, and notify on issues affecting ownership, transparency, privacy, and intention of collected personal data is a limiting factor in strengthening data ethics within the DevOps. Participants 1, 4 and 5 reported that there are no tools in place in their organisation for improving data ethics while participants 2 have tools that can enhance compliance (compliance as a code), participant 3 have in his organisation a data audit trail tool for review purposes, and participant 6 have a remote personal data deletion tool that strengthens data ownership by data subjects. Participants 1 and 2 strongly suggest the need for organisations to continuously strive to explore possibilities of automating processes that can enforce and review compliance to data ethics.

5.3 Data triangulation

The research has used data sources from mapped literature review and interviews. This helps to strengthen the validity and reliability of the research findings through corroboration. The validity of the factors influencing data ethics in DevOps practice holds true as factors identified from the mapped literature also reflects in the conducted interview. It can be deduced from both literature and interview that organisational culture towards data ethics is at low level as companies focus more on security. Also, the need for structured awareness and training program is reflected in both literature and interviews. The results of the interview and mapped literature also indicate that there is a weak data governance framework and oversight function which significantly affects data ethical practice and compliance in DevOps.

In addressing RQ1, both literature and interviews have suggested an effective awareness and training program to address this challenge of knowledge gap. However, none provided recommendations for the specific parameters to include in the program to enhance its effectiveness. For RQ2, literature highlighted importance of automated tools while interview mentioned few types in use at organisations that can enhance data ethics practice in DevOps. For RQ3, both emphasize the need to strengthen non-technical controls while the interview suggests separation of duties as an effective control in managing compliance. However, none provided effective control monitoring process. For RQ4, both suggest setting up a body that takes responsibility, provide oversight function, and demands accountability from officers implementing and managing data ethics related issues.

6 MITIGATION AND IMPROVEMENT STRATEGIES

The result of the analysis of literature review and interviews conducted clearly shows that there are pertinent challenges relating to data ownership management, transparency, and privacy in DevOps practice. The factors responsible for these deficiencies have been identified and validated through data triangulation. These identified factors responsible for the challenges affecting the adherence to good data ethical practices within DevOps is strongly anchored on the attitude of organisations adopting DevOps toward Data Ethics, the mindset of people hired into the DevOps team, robustness of awareness and trainings provided to DevOps teams on Data ethics as well as the organisational structures in place to ensure compliance to Data ethics.

Results from the research indicate that while some organisations are upscaling efforts towards achieving good data ethical practice, some are lackadaisical about it. Also, some of the approaches currently implemented are not robust enough to ensure high compliance. This is evident since majority of the respondent have poor visibility of Data Ethical practices in their organisation as majority confirmed that efforts are more geared towards security and much less of Ethical Data practice. This section discusses strategies that can be adopted and implemented to mitigate data ethical breaches as well as strengthen existing Data ethical practices in DevOps. These approaches that organisations can adopt are explained below.

1. **Strategically include data ethical considerations in organisational culture**

The role of organisations in driving ethical practice can not be overemphasized. The values organisation places on Data ethics goes a long way in ensuring the members of the DevOps team align appropriately. An organisation that is ethically bankrupt will influence the attitude and decisions of Data handlers in the DevOps team negatively while organisations with positive cultural values as regards ethics ensure the employees are properly aligned company's purpose. Senior management should make concerted effort in ensuring that Data ethics is deliberately included in the operational functions of the DevOps team.

The results of the interview conducted shows that while security receives lots of attention from management, data ethics is at the back burner. This lackadaisical attitude from management has the potentials to erode good ethical practices within DevOps and the organisation at large.

Regardless of the robustness of controls put in place to enforce compliance to data ethics, there is strong tendency for failure once the organisational behaviour or culture is weak. It is important for organisations with relatively small size to take data ethics seriously, as size of organisation is not a justifiable reason for non-compliance to statutory regulation.

Adequate measures should be put in place by organisations to ensure that DevOps team workload is distributed and balanced to avoid situations where work pressure introduces unethical data practices. It is also important for organisations to put in place a friendly workplace culture that encourages and reward DevOps team members who speak up when they encounter unethical conduct that can affect Data ethical practice. Organisations implementing DevOps must take into cognisance the compliance advisory responsibility they have as data processors to their clients who are the data collectors (Data Protection Ombudsman's Office, 2019). Instances where DevOps team members act on personal data unethically while working under pressure to satisfy client demand is unacceptable and a clear deviation from regulatory requirements.

2. Setup functional Data Governance Committee / Board

Result from the interview conducted shows that there are no clearly defined rules, expectations, procedures, roles, and responsibilities with respect to data privacy and compliance within DevOps practice and the organisation of some of the respondents. It is beneficial for organisations to set up a Data Governance committee that defines and oversees the governance framework of the organisation. The presence of a data governance committee ensures that (Collibra, 2021):

- Data from trusted sources is provided across the organisation.
- There is continuous effort in supporting availability, integrity, and usefulness of data.
- Available data is effectively used and not misused.
- Data policies are defined and implemented accordingly.
- Clearly defined procedures for data privacy, ownership and transparency compliance are established and monitored.

The purpose of the data governance framework is to support and ensure that the defined policies and rules pertaining to data is effectively enforced across the organisation. With proper implementation of the data governance, organisations will be able to demonstrate their

commitment to accountability of entrusted data. When designing the data governance framework, organisations should ensure that the following are catered for in the framework (Deloitte - Data Protection Control Framework, 2020):

- Processes that can routinely evaluate the operational effectiveness of the data ethics controls in place and perform corrective actions if necessary.
- Distinctly defined roles, responsibilities and communication/reporting channel that can enhance implementation of the controls.
- Key performance indicators that can be used to measure and monitor the effectiveness of the controls.

The Data governance committee managing the governance framework should be sufficiently independent from other entities in the organisation so they can execute their mandate in the organisation. There should be a dedicated individual at board level heading the data governance committee. This will help produce a powerful force, create more transparency, and allow data ethical issues get the required management attention. While some of the respondents confirmed that their organisations have a role dedicated to Data protection for the organisation, none of the respondent have a dedicated member in the DevOps team responsible for Data Ethics.

It is strongly suggested that a DevOps team member should be selected and trained as data ethics champion for the DevOps team. The member will be responsible for championing the cause of data ethics in the DevOps unit. He will also be on the look out for possible risk and areas that could cause data ethics breaches. This Data ethics champion from the DevOps team should serve as delegate to the data governance committee. All these efforts will help bridge the data ethics visibility gap in the DevOps team.

3. Incorporate data ethics in personnel screening, hiring, and onboarding process.

Humans continue to be the weakest link in policy and control implementation. The fabrics of data ethics is built around morals, behaviour, and trust. Results from analysis of the literature and interview indicate the possibility of a mischievous DevOps team member undermining compliance to data ethical practice. It is therefore essential that while organisation attempts to strengthen data ethical practice within the DevOps, the issue of hiring trusted personnels for the team is not treated with levity. As rightly mentioned by participant 4 that “it is difficult to handle data ethical issues

for those who intentionally decide to breach data for personal gains since the individual's mentality and intention really matter a lot in data ethics", still there are possibilities of minimizing these unpredictable impending actions of such unscrupulous team members. However, bringing a DevOps team member with malicious intention under control improves trustworthiness of data.

Organisations should ensure that beyond the technical competence of the job applicant, personality and character test should be administered during the screening process to confirm that the individual is the "right" candidate that fits into the ethical culture of the organisation. The more aligned the candidate's behaviour is to the organisational culture, the better the chances of the personnel adhering to laid down policies and procedures in the organisation. Extensive background check should be conducted to protect organisation and customers data from mischievous DevOps personnel.

The results from the interview indicate that often DevOps personnel are not exposed to data ethics training before they are granted access to organisation data. It is essential that at the time of onboarding and granting data access to the hired personnel, organisations conduct data ethics awareness and training for the DevOps personnel and ensure the new employee signs and agrees to understanding the data policies of the organisation as well as sign-off a non-disclosure agreement document (Saunders, 2021).

4. Implement Robust Data Ethics Awareness & Training Program for DevOps team.

Insufficient knowledge on data ethics and lack of structured awareness and training program for the DevOps team on data ethics have been identified from result analysis as one of the contributory factors for breaches and non-compliance. If users are not educated enough on the processes and procedure in place, there is a higher likelihood that an employee will make a mistake that may compromise data ethics. For organisations to achieve the desired result for Data ethics in the DevOps team and organisation at large, it needs to communicate the essentials of the program to its personnel. While some interview participants indicate that there are some trainings on Data ethics in their organisation, all participants agree the training is company wide and not specifically created for the DevOps team. It is important for organisations to create awareness and training program on Data ethics specific and targeted at the DevOps since this is a technical role.

DevOps team should receive a separate training that closely aligns with their daily task on data handling. This training should include several risk scenarios on how to identify and handle incidents of data ethical breaches. The awareness and trainings should be repeated in several formats such as login screen banners, posters, employee handbook, online and in-person live training. Also, organisations can include gamification into the awareness training program. This involves applying game elements in non-game related situations for the purpose of improving learning. Gamification has the tendency of greatly increasing employees skills retention (Simpson & Jenkins, 2015).

Data ethics awareness training should be periodic, and its content be reviewed appropriately to reflect current industry happenings. The expected obligation and tolerable behaviour from the DevOps team members on data ethics must be clearly defined and communicated during the training. Also, the repercussions for non-compliance should be discussed and trainees should be made to sign that they clearly understand and agree to the terms and conditions on Data ethics discussed in the training.

At the end of the training, it is essential to evaluate its effectiveness. Participants can be asked to take a short test to confirm they truly understand the content. Another method is to conduct a social engineering test and data integrity drills that can confirm if the DevOps team understands, is continuously conscious and can apply the elements of the Data ethics training in their daily task. In event that a team member fails the various types of tests, it is important that the feedback is delivered constructively to the affected member, to improving their ethical behaviour and achieve greater positive results subsequently. Overall, based on the finding of the research, it is anticipated that a formalised and structured process of data ethics awareness training for the DevOps team can sufficiently improve DevOps personnel behaviour and perspective towards data ethics.

5. Implement issue-specific policies and controls for Data ethics.

Having a policy in place that specifies the rules and expectation on how data is collected, stored, used, and deleted in the organisation is essential for establishing data ethical practice in DevOps and organisation as a whole. All the interview participants affirmed that they are unaware of any Data policy in place in their organisation. It is suggested that Data policies should be issue-specific for the DevOps operation and focused on access, usage, and accuracy of data especially as it affects

laws, regulations, and all applicable business obligations. Policy should be simple to understand for the DevOps team, easily accessible for reference purpose and should be reviewed often in response to changes in regulatory and business compliance requirements.

The purpose of control is to prevent, detect, contain, or recover from an incident. The result of analysis of the different risk factors of data ethics in DevOps will determine the type of control an organisation will put in place to check-mate and respond to data ethical breaches. Appropriate controls should be selected and implemented to enforce compliance to Data ethics. The leaning of Data ethics more on the side of morals and behaviour makes only technical controls to be insufficient. There should be a blend of both technical and non-technical control in combating data ethical breaches.

For non-technical controls, the application of separation of duties where more than one individual is required to perform a task is an effective way of preventing malicious data ethical breaches in DevOps. None of the users has absolute privilege sufficient to significantly abuse the entire process. One person must review and approve the task of the other person before it gets to completion. Background checks, non-disclosure agreements, training, openness, and speak-up culture are all non-technical or administrative controls that can enhance data ethics in DevOps.

For the technical controls, the use of digital technologies or equipment is involved. Participant 2 confirmed that the organisation has compliance-as-code tool integrated in their software development process to prevent, detect, and remediate non-compliance to relevant policies and regulations. Also, participant 5 informed that there is a software tool in their organisation that allows users to delete their personal data remotely thereby improving data ownership. Even though the result of the research shows that it can be difficult to have an effective digital tool that can holistically support Data Ethics in DevOps, however tools such as Data classification software which can identify and classify sensitive data in the organisation as well as Data Loss Prevention (DLP) software tools which ensures confidential data is not lost, abused, or accessed by unapproved persons are efficient in addressing Data ethics privacy and protection challenges. With the use of DLP tool in DevOps, the organisation can comply with some data laws and regulations such as GDPR that mandates organisations to (Coos, 2022):

- Detect where personal data is stored.

- Remove personal data when it is no longer required.
- Regulate the usage of personal data.
- Prevent unauthorised changes and loss to personal data.
- Support security standards for personal data.

Some common DLP software tools in the market that organisations can consider for use include (Cooper, 2019):

- SolarWinds Data Loss Prevention tool
- ManageEngine Endpoint DLP
- Symantec Data Loss Prevention
- ManageEngine Device control
- ThreatLocker

6. Setup effective communication and reporting channel.

There should be a clearly defined communication and reporting channel for issues bother on Data Ethics. All participants interviewed confirmed that there are no reporting and escalation procedures in place for issues affecting Data ethics within DevOps. It is suggested that there should be a direct communication between members of the DevOps team and the Data protection officer in the organisation. Instances where DevOps team members must initially discuss or seek permission from a senior member of the team before escalating unethical practice must be discouraged as this could result in conflict of interest.

These reporting channels for unethical data practices should be included in the policy document as well as explained during awareness training sessions. One important and effective way of reporting anomalies in ethical conduct is whistle blowing. With a whistle blowing program in place, DevOps members can anonymously report unethical conducts pertaining to personal data. It is important for the organisation to put in place adequate protection for the whistle blower and all reports should be handled with upmost secrecy.

7. Monitor & Measure Policy compliance and Control effectiveness.

To ensure adequate compliance to policies, there should be in place mechanism to monitor and measure the data ethics controls implemented in the DevOps team and organisation in general. The

essence of monitoring the control is to confirm that the control activities effectively address the risk associated with the data ethical breaches. With continuous monitoring of the controls, the responsible personnel for data ethics is able to confirm if the controls are operating in tandem with defined performance targets. Log files providing historical records of activities of the control in place to mitigate data ethical breaches should be kept. It is essential for the information kept in the log file to be in a comprehensible format. Monitoring and analysing the log files can alert organisations of deviation from norms. An audit team should also be involved to provide an independent and unbiased opinion on the efficacy and suitability of the control environment. When incidents of non-compliance or underperformance is detected, adjustment, enforcement, or complete implementation of new policy and control should be performed.

Key performance indicators (KPI) should be defined to measure how much the controls deviate from the expected goals. KPI provides specific, measurable, and quantifiable metrics that can be used to monitor and track performance progress over a period of time (Jackson, 2022). The number of personnels that have attended the data ethics awareness training, the number of data ethical incidents reported by DevOps team members, the time between when incident occurred and when it was reported, the number of unresolved alerts in the DLP and other data ethics compliance tools are some of the places where measurement can give useful insight on actions to take before a significant undesirable impact arise.

8. Continuously review policies and controls

The number of data-related regulations in the global space keeps increasing. Table 1 shows some out of the several global data protection laws. These variations and contradictions in laws from one country to another makes it difficult for organisations whose business operations cuts across the globe to respond to changes in international regulations and emerging laws which may be unknown. It is essential for organisations to constantly evaluate and make changes to their data ethics policies and controls in order to reflect and align with changes in data laws of their jurisdiction of operation. To overcome the challenges of keeping up with varying global laws, organisations whose business operate across different regions can develop a data ethics policy and control suite that can address common global regulatory requirements, and thereafter can have a country or region-specific policy and control in addition to the suite to be able to cater for the exceptions or conflicts (CRISC review manual, 2021).

7 ARTIFACT DEVELOPMENT AND EVALUATION

The section describes a model for the implementation of an operational data ethics framework for the DevOps practice. An evaluation of the model is also performed using industry experts in audit, risk, compliance, and information systems control design, to appraise the suitability of the model for use in DevOps.

7.1 Model Development

The model consists of several link stages to achieve a robust framework that optimally support the implementation of Data ethical practice in DevOps. A data governance committee is put in place to dictate the roles, responsibilities, policies, and controls for the data ethics program. The committee reports to the Board of the company and performs oversight function on how data is collected, kept, used, and discarded. A member of the DevOps team designated as "data ethics champion" represents the DevOps team in the committee.

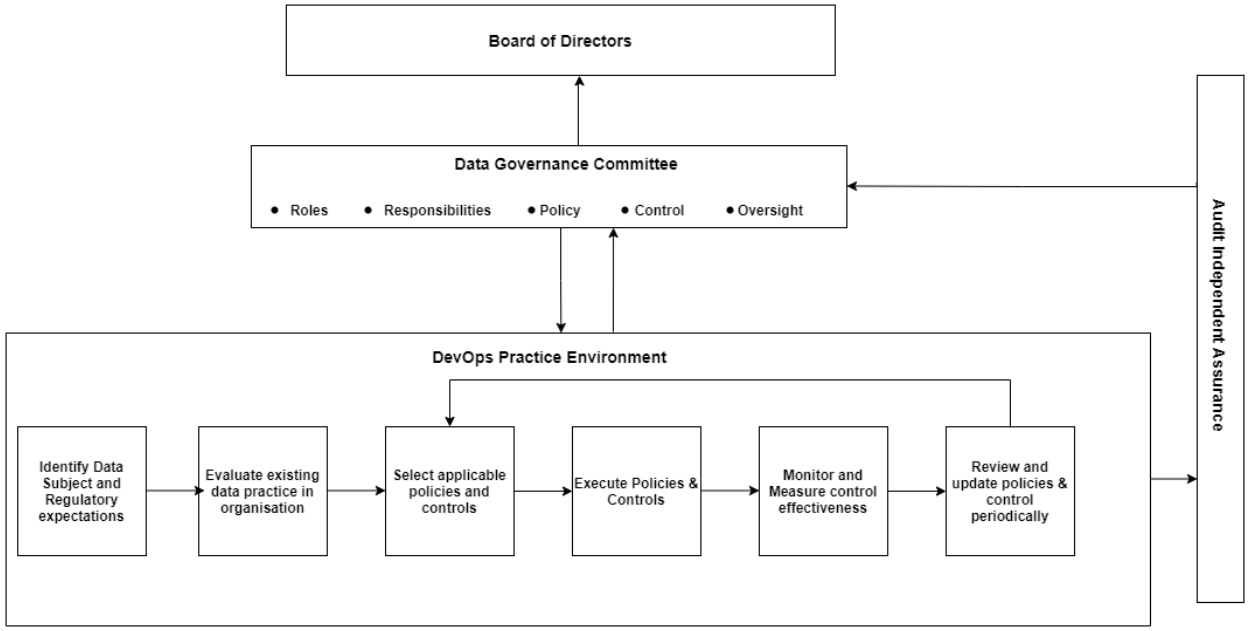

Figure 5: Process Model for implementation of Data Ethics framework in DevOps

Within the DevOps environment, the expectations of the Data subjects and that of Regulatory bodies are first identified. This will provide a clear understanding on how the customers want their data to be treated as well as the mandatory requirements that must be adhered to in data handling.

After a clear understanding on the expected data handling approach, the next is to appraise the current situation with respect to what data is collected, how the collection process is carried out and where it is stored and as well as used. This evaluation stage should be carried out with all relevant data stakeholders across the organisation. The findings of the evaluation will determine the need or otherwise for process adjustment or improvement.

Based on the outcome of the evaluation, appropriate data ethics policies and controls defined by the data governance committee is selected and implemented in the DevOps environment. The policies and controls now in place are continuously monitored and measured for operational effectiveness. The data ethics policies and controls in use are then subjected to periodic review in accordance with regulatory compliance and customer expectation. The result of the review may necessitate selection of new controls which is to be defined by the governance committee. The compliance to the policies and controls within the DevOps environment is independently validated by an Audit team and the report of the findings is communicated to the Data governance committee who ensures non-conformities identified by the audit team are corrected.

7.2 Model Evaluation

The proposed process model along side the mitigation and improvement strategies discussed in chapter 6 were shared with two industry experts to get informed opinion on the feasibility of implementation in a DevOps environment. Both experts have more than 15 years industry experience in planning, implementing, monitoring, and auditing policies and controls within IT environment. One of the selected experts also doubles as a software engineer with ample experience within agile and DevOps environment. The intention of the evaluation is to see how suitable the model is in addressing RQ3 *"What are the effective controls, monitoring and reporting channel for Data ethical problems within the DevOps team and organisation?"* and RQ4 "*Who should be responsible and accountable for ethical data practices in the DevOps team and organization?".*

Both industry experts agree that setting up a data governance committee provides a holistic approach to managing data ethics in the organisation and that a representative from the DevOps team into the committee will help strengthen Data ethics in DevOps. They are however of the

opinion that the role of data protection officer in the organisation should not be overshadowed by the Data governance committee. The committee should be responsible for ensuring data ethics compliance while the data protection officer should be tasked with executing the mandate of the committee and be accountable to the committee. One of the experts also indicated that DevOps results in strong collaboration between the two traditional independent teams. This collaboration can a times be effected in collaborative physical workspaces to improve communication. The expert opined that this could result in unapproved data exposure between collaborating members. This agrees with one of the reasons given for data ethical breaches in DevOps by interview participant P4 that *"sometimes team members need help from each other and in the process of requesting or receiving help, other members who ideally have not been setup to have access to specific data may end up knowing what they are not supposed to know"*. The expert suggests implementing physical controls such as workspace segregation and separation as well as clean desk policy in DevOps environment.

The audit expert also suggest that the audit charter and plan used by the Audit team for validating the data governance process should be approved by the board and not the data governance committee who has a reporting responsibility to the board. He informed that there should not be any form of interference in determining the scope of audit work and in cases where there are any of such meddling, the head of audit team should disclose and discuss the implications to board of directors. All of these are aimed at strengthening the independence of the audit process. Overall, both industry experts agree that the process model and mitigation/improvement strategies highlighted in the research are useful in enhancing Data ethics and compliance in the DevOps environment.

8 DISCUSSIONS

This chapter discusses the outcome of the literature review and interview as well as the findings from the research. It goes further to show the comparison between the findings of the research and previous works indicated in the literature review. The validity of the research is also discussed while limitations to the research conducted and future improvement possibilities for the conducted research are suggested.

8.1 Discussion

Selected studies reflected in the literature review have emphasized the importance of awareness of data ethics among DevOps team members (Skenderi et al., 2020; Floridi & Taddeo, 2016). While Skenderi et al. (2020) is of the opinion that coders have high level of awareness on what data ethics is, the researcher further informed that there still exist a significant level of knowledge gap on ethics among team members working within DevOps environment. This revelation of gaps informed the RQ1. *Are programmers and operations team aware of data ethical issues and its implications?*

Findings from the research interview shows that even though the interviewees are familiar with the principles of data ethics which includes privacy, ownership, and transparency, thereby corroborating the claims of sufficient awareness indicated in the literature review, majority of the respondents found it difficult to separate data ethics and data security. All the respondents were initially of the opinion that both concepts of ethics & security can be used interchangeably. Despite the narrow division between the two, there still exist significant difference as data ethics is more about moral obligations on data usage whose responsibility falls more on internal members of the organisation handling data as against security which is usually considered as external threat.

The result of the research reveals that this muddle up of data ethics and security is basically because most organisations do not have trainings dedicated to data ethics and rather only discuss it during data security trainings to staff members. Confidentiality of data which is one of the information security triads is only one of the several objectives that data privacy/ethics is meant to achieve. Combining both security and data ethics training program usually reduces the effectiveness of the later and makes the two distinct concepts appear as same.

Furthermore, while the literature review has suggested trainings as a potent measure towards preventing non-compliance to data ethics, this research has further revealed the appropriateness of time in incorporating the training and awareness programs as an important factor to consider. The findings of the research shows that data ethics is usually not included in the recruitment and onboarding process. The training & awareness sessions usually come only after the DevOps personnels have commenced work and are already exposed to personal data in the organisation. This is a case of "putting the cart before the horse" and the implications can be very detrimental to the organisation especially when onboarding DevOps personnel who are novice and have not received any prior trainings on data ethics. Improvement strategies for conducting adequate trainings and awareness programs as well as how data ethics can be incorporated in personnel screening, hiring, and onboarding process for the DevOps team is detailed in chapter 6.

While the literature review reiterates the importance of incorporating the automated tools that can track compliance to data ethics into the DevOps process, Abrahams & Langerman (2018) in the review is of the opinion that software tools can not be used to automate non-technical or personnel-based regulatory compliance processes within the DevOps environment. This is the premise on which the RQ2. *What tools and processes are available to identify data ethical concerns in DevOps?* is based.

Some of the interview participants raised their doubts on the possibilities of automating a behavioural process such as data ethics thereby aligning with the thoughts of Abrahams & Langerman (2018) in literature review. However, the outcomes of the research confirmed by other interview participants shows that software tools that brings about these capabilities are available and in use in the industry. These includes compliance as a code, identity governance & administration (IGA) tools which allows for integration and enablement of separation of duties within the DevOps environment as well as disaster loss prevention tools which greatly enhances data ethical practices. The research findings further show that these tools are often used by organisations of large sizes and those embarking on projects within heavily regulated environments.

The literature review emphasized the importance of having in place controls to enforce compliance. The research investigated existing controls in DevOps practice and attempted to find

out their suitability in the *RQ3. What are the effective controls, monitoring, and reporting channel for Data ethical problems within the DevOps team and organization?* The research findings show a lackadaisical attitude of management towards data ethics. A sizeable number of the respondents indicated that their organisations focus more on security and data ethics is not discussed. Three (3) interview respondents informed that the only control they are aware of in their organisation is training while the others informed that they are not aware of any controls relating to data ethics.

Also, all the participants are unaware of any method used to appraise or monitor control performance in their organisations. They all have also not been exposed to any data ethics policy document or framework in place in their organisations while they have been informed about the organisation's security policies several times. These findings show that organisations culture with respect to data ethics remain poor. Organisations must embrace the reality of the consequences of data ethical breaches and put in place effective technical and non-technical controls. There should also be mechanisms in place to continuously monitor the performance of these controls. For technical controls, integration of digital tools into DevOps has been suggested in the improvement strategy section (chapter 6) while segregation of duties, background checks, non-disclosure agreements, training, openness, and speak-up culture have been listed as non-technical or administrative controls that can enhance data ethics in DevOps.

Results from the literature review suggest that lack of human oversight in automated systems can result in abuse of personal and sensitive data. The research investigated the organisational structure in place in DevOps environment to address Data ethics compliance and mitigate breaches by addressing the RQ4. *Who should be responsible and accountable for ethical data practices in the DevOps team and organization?* The research result shows that some organisations have data protection officer dedicated to data ethics in their organisation while others do not. Also, none of the respondents have any personnel dedicated to data ethics related issues in the DevOps team in their organisation.

The respondents are also not aware of escalation matrix and reporting channels in place in their organisation for data ethical breaches. The findings of the research reveal that establishing a data governance committee tasked with the responsibility of executing the organisation's data governance framework and appointing a data ethics champion for the DevOps team with the

responsibility of advancing the cause of data ethical practice in DevOps will be an effective approach towards improving oversight function and enhancing data ethical practices in the DevOps team and organisation.

In general, outcomes of this study strongly indicate that improving data ethics and compliance within the DevOps practice is deeply influenced by the attitude the organisation implementing DevOps have toward Data Ethics, the mindset for ethical practice of people hired into the DevOps team, the adequacy of data ethics awareness & trainings provided to DevOps teams as well as the organisational structures and controls in place to enforce compliance to data ethics.

8.2 Validity of Research

The intention of this section is to demonstrate that the research conducted is rigorous and the outcome is trustworthy. This involves providing evidence that the way the research is designed is able to provide answers to the research question and adequately discourse the research topic. To convincingly provide this evidence, the research is examined against the following:

Construct validity: The Semi-structured interview has been designed in a way that both the interviewer and interviewees have a common understanding of the language of communication. Interview questions was drafted based on McIntosh & Morse (2015) interview guideline and the participants were provided scaled-down checklist of areas of discussion prior to the interview to make them familiar with the key concepts to be discussed.

External Validity: This measures the extent to which the result of the research can be extended or generalized. The interview participants are carefully selected to represent different geographical locations across Europe, North America, and Africa. Also, the participants work in diverse industry cutting across software development, consulting, and manufacturing. The sizes of these organisations also differ. This allows the outcome of the research to be scalable and applicable to varying situations.

Confirmability: This provides evidence that the result can be authenticated or endorsed by others. The model and suggested mitigation strategies have been shared with industry experts and they agree with the findings of the research. Also, the interview transcript has been included into this

report to confirm the reliability of the research.

Credibility: This shows the extent to which the research is trustworthy and believable. There is a common view expressed by the interview participants on the factors that are responsible for data ethical issues in DevOps. This shows that the result is credible else the degree of divergence in opinions would have been wide. Also, the factors identified by the interview participants are similar to those identified in the mapped literature review. This goes further to provide credibility and make the results of the research convincing.

8.3 Limitation and Future work

The database from which the research literature is obtained are google, google scholar and IEEE Xplore digital library. Limiting our information source to these three search engines could have sufficiently limited the amount of information and resources on Data ethics within the DevOps practice. Also, only six participants were considered during the interview process. Increasing the number of interview participants may have identified other factors that can be responsible for Data ethical breaches and non-compliance in DevOps. Also, administering surveys questionnaires to a larger population could have expanded the response received, increased the statistical power as well as further strengthen the credibility of the research. The participants are also drawn only from those working in DevOps teams. Interviewing a senior management personnel or a data protection officer could have shed more light on how organisational culture and oversight functions affects data ethics in their organisation.

It is recommended that researchers interested in furthering this area of research can study why managements in organisation channel more resources to security and less consideration given to Data ethics. This will focus the research more on the management and not the DevOps team. Researchers can also design a tool that integrates all the mitigation and improvement strategies identified in this study. This will go a long way in harnessing all the solutions into a single product that can be used by organisations and advance the cause of data ethics in DevOps. Also, an open-source contribution platform can be developed so that individuals practicing DevOps in their organisation can identify other factors that can affect data ethics in DevOps practice and suggest other improvement strategies. This will further strengthen Data ethics in organisations adopting DevOps practice.

9 CONCLUSIONS

The need to embrace data ethics in software engineering practice is evident considering the likelihood of data breaches driven by the continuous growth in the number of customers' personal information that is collected and processed by data handlers. Data ethics puts in place a standard of trust between data subjects and processors. DevOps methodology which is one of the most used software development models increases the capacity of organizations to deliver applications and services at increased speed by improving the communication and collaboration between the development and operations team. In this report, the challenges of implementing Data ethical practices in DevOps are examined.

The literature review in the research attempted to examine previous works done on the research topic and research questions. The evolution of DevOps and its practices and significant difference from other software engineering practice models was explored. Afterwards, background knowledge on data ethics was identified from literature. The research further advanced by exploring existing literature works on data ethics within the DevOps practice. Thereafter relevant research works that address the research questions were identified and analyzed. The overall objective of the literature review is to provide answers to the research questions. An interesting observation that can be seen from the literature review is that the works did not provide extensive explanation for each of the suggested answers provided.

To corroborate the results of the mapped literature review, a semi-structured interview was performed. Relevant interview questions capable of providing answers to the research questions were developed and Participants with DevOps knowledge were drawn from the industry. Thematic analysis is performed to explore and interpret patterns in the obtained interview dataset. The result from the thematic analysis shows a strong linkage to those factors also identified as being responsible for Data ethical breaches in DevOps in mapped literature review. This linkage is explained more in the data triangulation performed in chapter 5.

Lack of knowledge on Data ethics and inadequate data ethics awareness training program for DevOps team members is the most significant of all the identified factors that can affect data ownership, transaction transparency, consent, and privacy according to both literature and interview participants. This places a burden of responsibility on organizations to identify the right

personnel that can work and adhere to data ethical practices within the DevOps practice.

The research outcome indicate that majority of DevOps team members are aware of basic concepts of data ethics and the implication of non-compliance. However, despite this awareness, the organizational culture where they work does not provide a platform that can support them in being aligned to data ethical practices. Discussion and consideration for data ethics is often not included in the recruitment and onboarding process in most organizations. The research findings further show that there is a thin line of division between security and data ethics in most organisations, training is tilted towards security and little or no focus on data ethics. This poor organizational culture alongside lack of automated tools to ensure compliance to data ethics, non-existent data governance framework, work pressure that can result in compliance negligence are part of the factors that raises data ethics concern within DevOps practice.

This report has extensively identified several of the factors responsible for data ethical breaches in DevOps practice. Mitigation and Improvement strategies on how these identified challenges can be managed have been suggested. Organizations must put in place effective controls that can enforce compliance with data ethical practices, detect breaches and correct or prevent occurrence. Beyond implementing controls, it is also important to have capabilities to continuously monitor and measure performance of these controls. It is important to keep auditable log files that can show patterns of event and non-compliance to ethical practice.

Key performance indicators should also be clearly defined to measure control performance against expected values. Activities to address these needs have been discussed in the report. The importance of having a strong oversight of all the activities in place cannot be overemphasized. In the report, it is suggested that a Data governance committee should be put in place to define and execute the data governance framework of the organization and see to it that it is effectively implemented in the DevOps team.

To be able to effectively define, analyze and communicate the concept of implementing a successful data ethics program in the DevOps environment, a model has been designed and evaluated for performance. The model shows a process flow on activities to be carried out to implement a data ethics framework and enhance data ethics in DevOps. The need for effective controls, oversight functions, independent audit process and reporting functions have been clearly

captured in the artefact. This model, when used in conjunction with the mitigation strategies can remarkably advance the cause of data ethics within DevOps practice and the organization.

Practitioners of DevOps who are currently faced with problems associated with non-compliance to data ethics can benefit enormously from the information provided in this thesis report while those who are yet to adopt DevOps can as well use the research findings as precautionary guidelines when they eventually decide to embrace DevOps practice. Even though the research has been carried out with much focus on DevOps, it is strongly believed that the outcomes of the research can be extended to other organizational practices where there is a need to provide guidelines on how personal data is collected and manipulated.

REFERENCES

5 Principles of Data Ethics for Business. (2021, March 16). Business Insights Blog. https://online.hbs.edu/blog/post/data-ethics

Abrahams, M. Z., & Langerman, J. J. (2018). Compliance at Velocity within a DevOps Environment. *2018 Thirteenth International Conference on Digital Information Management (ICDIM)*, 94–101. https://doi.org/10.1109/ICDIM.2018.8847007

Atlassian. (n.d.). *What is DevOps?* Atlassian. Retrieved 12 July 2022, from https://www.atlassian.com/devops

Baskerville, R., Pries-Heje, J., & Venable, J. (2009). Soft design science methodology. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, 1–11. https://doi.org/10.1145/1555619.1555631

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Caulfield, J. (2019, September 6). *How to Do Thematic Analysis | Step-by-Step Guide & Examples*. Scribbr. https://www.scribbr.com/methodology/thematic-analysis/

Cooper, S. (2019, April 18). 10 Best Data Loss Prevention Tools & Software. *Comparitech*. https://www.comparitech.com/data-privacy-management/data-loss-prevention-tools-software/

Coos, A. (2022, June 14). Top 5 Ways DLP can help with GDPR compliance. *Endpoint Protector Blog*. https://www.endpointprotector.com/blog/top-5-ways-dlp-can-help-with-gdpr-compliance

Data governance council: What is it and why do you need one? (n.d.). *Collibra*. Retrieved 3 March 2023, from https://www.collibra.com/us/en/blog/data-governance-council-what-is-it-and-why-do-you-need-one

Dingsøyr, T., Nerur, S., Balijepally, V., & Moe, N. B. (2012). A decade of agile methodologies: Towards explaining agile software development. *Journal of Systems and Software*, *85*(6), 1213–1221. https://doi.org/10.1016/j.jss.2012.02.033

Director, R. H., Iheanacho, I., Payne, K., & Sandman, K. (n.d.). *What's in a Name? Systematic and Non-Systematic Literature Reviews, and Why the Distinction Matters*. 2.

DLA Piper Global Data Protection Laws of the World—World Map. (n.d.). Retrieved 13 July 2022, from https://www.dlapiperdataprotection.com/

Ethical data usage in an era of digital technology and regulation | McKinsey & Company. (n.d.). Retrieved 24 August 2022, from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-forward/ethical-data-usage-in-an-era-of-digital-technology-and-regulation

Farroha, B. S., & Farroha, D. L. (2014). A Framework for Managing Mission Needs, Compliance, and Trust in the DevOps Environment. *2014 IEEE Military Communications Conference*, 288–293. https://doi.org/10.1109/MILCOM.2014.54

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160360. https://doi.org/10.1098/rsta.2016.0360

GDPR - Data Protection Control Framework. (n.d.).

Guo, J., Yang, M., & Wan, B. (2021). A Practical Privacy-Preserving Publishing Mechanism Based on Personalized k-Anonymity and Temporal Differential Privacy for Wearable IoT Applications. *Symmetry*, *13*(6), Article 6. https://doi.org/10.3390/sym13061043

Hand, D. J. (2018). Aspects of Data Ethics in a Changing World: Where Are We Now? *Big Data*, *6*(3), 176–190. https://doi.org/10.1089/big.2018.0083

Hevner, A., R, A., March, S., T, S., Park, Park, J., Ram, & Sudha. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly*, *28*, 75.

Ibrahim, M. (2012). *THEMATIC ANALYSIS: A CRITICAL REVIEW OF ITS PROCESS AND EVALUATION*. *1*(1).

Jackson, T. (2022, April 22). 30 KPIs To Measure Performance (& How To Choose & Track Them). *ClearPoint Strategy*. https://www.clearpointstrategy.com/18-key-performance-indicators/

Johnson, B., & Smith, J. (2021). Towards Ethical Data-Driven Software: Filling the Gaps in Ethics Research & Practice. *2021 IEEE/ACM 2nd International Workshop on Ethics in Software Engineering Research and Practice (SEthics)*, 18–25. https://doi.org/10.1109/SEthics52569.2021.00011

Laukkarinen, T., Kuusinen, K., & Mikkonen, T. (2017). DevOps in Regulated Software Development: Case Medical Devices. *2017 IEEE/ACM 39th International Conference on Software Engineering: New Ideas and Emerging Technologies Results Track (ICSE-NIER)*, 15–18. https://doi.org/10.1109/ICSE-NIER.2017.20

Lazarsfeld, P. F. (1935). The Art of Asking WHY in Marketing Research: Three Principles Underlying the Formulation of Questionnaires. *National Marketing Review*, *1*(1), 26–38.

Leech, B. L. (2002). Asking Questions: Techniques for Semistructured Interviews. *PS: Political Science & Politics*, *35*(4), 665–668. https://doi.org/10.1017/S1049096502001129

Macarthy, R. W., & Bass, J. M. (2020). An Empirical Taxonomy of DevOps in Practice. *2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 221–228. https://doi.org/10.1109/SEAA51224.2020.00046

Magaldi, D., & Berler, M. (2020). Semi-structured Interviews. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of Personality and Individual Differences* (pp. 4825–4830). Springer International Publishing. https://doi.org/10.1007/978-3-319-24612-3_857

Majluf, N. S., & Navarrete, C. M. (2011). A Two-Component Compliance and Ethics Program Model: An Empirical Application to Chilean Corporations. *Journal of Business Ethics*, *100*(4), 567–579. https://doi.org/10.1007/s10551-010-0696-6

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Marks, D. F., & Yardley, L. (2004). *Research Methods for Clinical and Health Psychology*. SAGE.

McIntosh, M. J., & Morse, J. M. (2015). Situating and Constructing Diversity in Semi-Structured Interviews. *Global Qualitative Nursing Research*, *2*, 2333393615597674.

https://doi.org/10.1177/2333393615597674

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. SAGE.

Namey, E., Guest, G., Thairu, L., & Johnson, L. (2008). Data reduction techniques for large qualitative data sets. *Handbook for Team-Based Qualitative Research*, *2*(1), 137–161.

Oh, S.-R., Seo, Y.-D., Lee, E., & Kim, Y.-G. (2021). A Comprehensive Survey on Security and Privacy for Electronic Health Data. *International Journal of Environmental Research and Public Health*, *18*(18), 9668. https://doi.org/10.3390/ijerph18189668

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Processors' responsibilities | Data Protection Ombudsman's Office. (n.d.). Tietosuojavaltuutetun Toimisto. Retrieved 3 March 2023, from https://tietosuoja.fi/en/processors-responsibilities

Ramaj, X., Sánchez-Gordón, M., Gkioulos, V., Chockalingam, S., & Colomo-Palacios, R. (2022). Holding on to Compliance While Adopting DevSecOps: An SLR. *Electronics*, *11*(22), Article 22. https://doi.org/10.3390/electronics11223707

Saunders, A. (2021, November 19). How to implement an actionable data ethics framework. *TechCrunch*. https://techcrunch.com/2021/11/19/how-to-implement-an-actionable-data-ethics-framework/

Service, U. D. (n.d.). *Qualitative data*. UK Data Service. Retrieved 23 January 2023, from https://ukdataservice.ac.uk/learning-hub/qualitative-data/

Simpson, P., & Jenkins, P. (n.d.). *Gamification and Human Resources: An overview*.

Skenderi, M., Luma-Osmani, S., & Imeri, F. (2020). ETHICS IN DevOps, THE ATTITUDE OF PROGRAMMERS TOWARDS IT. *Journal of Natural Sciences and Mathematics of UT*, *5*(9–10), Article 9–10.

Talking data ethics: What it is and why it's important. (n.d.). *Collibra*. Retrieved 25 August 2022, from https://www.collibra.com/us/en/blog/talking-data-ethics-what-it-is-and-why-its-important

Team, K. P. N. (n.d.). *Traditional vs. Agile Software Development Methodologies*. Retrieved 7 July 2022,

from https://www.kpipartners.com/blog/traditional-vs-agile-software-development-methodologies

Van der Merwe, A., Gerber, A., & Smuts, H. (2020). *Guidelines for Conducting Design Science Research in Information Systems* (pp. 163–178). https://doi.org/10.1007/978-3-030-35629-3_11

Venable, J. R., Pries-Heje, J., & Baskerville, R. L. (2017). Choosing a Design Science Research Methodology. *ACIS 2017 Proceedings*. https://aisel.aisnet.org/acis2017/112

Virmani, M. (2015). Understanding DevOps & bridging the gap from continuous integration to continuous delivery. *Fifth International Conference on the Innovative Computing Technology (INTECH 2015)*, 78–82. https://doi.org/10.1109/INTECH.2015.7173368

Why Data Ethics are Important for Your Business. (2022, May 25). IT Business Edge. https://www.itbusinessedge.com/business-intelligence/data-ethics-framework/

Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering*. Springer.

Zhu, L., Bass, L., & Champlin-Scharff, G. (2016). DevOps and Its Practices. *IEEE Software*, *33*(3), 32–34. https://doi.org/10.1109/MS.2016.81

Michelle, K. (2021). *What is Data Ethics?* Retrieved 13 July 2022, from https://www.dataversity.net/what-are-data-ethics

Vaishnavi, V., & Kuechler, W. (2015). *Design Research in Information Systems* (January 20, 2004, Last updated November 24, 2021). Retrieved August 29, 2022 from http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf.

APPENDIX

Appendix 1: Transcribed Interview data.

Table 6. Interview conversation with Participant 1

Participant 1 [P1]	DevOps Engineer
Years of Experience within DevOps	3 years
Does your organisation develop solutions for diverse clients across the globe or is it limited to a specific geographical location?	For the company I work with right now, it is only some selected geographical location. Our products are focused on the American and European markets. we have solutions that falls within regulated standards such as Internet of Things. We have solutions in large scale for industrial IoT. We make solutions for Elevators which are governed by regulatory standards.
What does DevOps mean to you and to what extent is it being practiced in the organisation you work with?	For me, DevOps is a culture to be honest. And what I meant by saying it is a culture is that it cuts across all set of engineering. In software engineering where we have the software development lifecycle, we interact between developers and operations, and we want the interaction to be much smoother and that is where DevOps came about. Technology is advancing and we have moved on from the slow-paced traditional waterfall software development model. Now we want to have faster code and want to change something on the go and DevOps brings these possibilities. In my own company, we are practicing DevOps in our own software development. We want to meet up with the demand of the clients and ship our code much faster, so we need the DevOps way of working in the company.
What does data ethics mean to you?	So, for me, as a DevOps engineer what I understand by data ethics is the need to protect data of the employee, employer, and our customers at all times. We work in compliance with GDPR rules in Europe and relevant data laws in the America. We always try to be data compliant. We have our data protection officer who try to understand the country laws about data before we can provide solution for any region, we want to operate in. So as DevOps professionals, we try to keep the data we work with as discreet as possible since we are bounded by the law and non-disclosure agreement we have with the company. In my company, the DevOps engineer do not even have access to real data. We mostly work on data that is unreadable so that we do not get to have unauthorized access to client's data. As DevOps Engineer, I also ensure the pipelines and platforms are encrypted.
What are the business benefits of adherence to ethics of data usage and implications of data ethical breaches?	Well, the major benefit that comes to my mind is securing the trust of the customer and of course this means the customer base will continue to grow and business profit as well. What most companies are selling now is Data driven and there is strong need to ensure the data is handled properly. for cases of breaches there are penalties from the regulatory bodies. Reason a lot of efforts are being channeled into data privacy issues.

What are the obstacles to achieving high level of data ethics within the DevOps practice?	Okay. In DevOps we preach more about Security and hardly on ethics. The trainings are more about security awareness. I think either ethics or security the main factor is when the DevOps personnel is not properly trained or aware of what to do then there can be these ethical or security breaches. Also, sometimes the Developers put so much pressure in DevOps engineers and this can lead to data ethical breaches.
Have you found yourself in situations where you needed to compromise on data ethics while attempting to optimize release frequency and velocity?	Well, I have found myself in those situations especially. But as an engineer who is properly trained especially in my previous job, I do not compromise. Also, in my company we have senior members of the team who are dedicated to checking to ensure there are no data compromise before things get into production. But not every industry or company does this practice because I am aware in some companies these extra checks are not in place.
Does your organisation and DevOps team have a staff role dedicated to and accountable for Data Ethics?	There is none dedicated to such within the DevOps team. But the Data protection officer for the company oversees all issues bothering on compliance and Ethics.
Who is primarily responsible for Data Ethics and Privacy in your organisation.	I do not know who takes responsibility. Maybe the Data protection officer
How does your organisation ensure compliance to Data ethical and privacy laws and regulations for multiple global projects?	We have data protection officers and security officers that communicate with us and have us trained and lots of meeting with us in DevOps. They have tools they use to scan for vulnerabilities and if issues are found we are informed. Like I mentioned earlier, we deal more with security, the company invest more in fencing off external threats to our operation, and I think if security is properly taken care of then data ethics should be in good standing too. I may be wrong anyway.
Is there a data ethics policy and data governance framework in place in your organisation and are you aware of the content of the policy and the framework?	None that I am aware of. There may be but I have not been privileged to know or hear about it.
What are the data ethics control and reporting processes in place in your organisation to mitigate against data ethical issues within the DevOps practice?	We have training materials we read for compliance, ethics, and security. It is handled by our Data protection officer, and this happens every quarter. This is the process I know in place.
How does your organisation measure and monitor the effectiveness of the controls?	We just read the training materials. I do not know if there are ways effectiveness is measured or monitored. Maybe the data protection officer does it, but I am not privy to these things.

Are there formal data ethics awareness trainings in your organisation for DevOps team and how frequently is it conducted?	Well, it is not a formal training dedicated to Data Ethics or specifically for the DevOps team. It is same training for everyone in the organisation. Maybe the senior managers have separate training, but I do not know. The training is pre-recorded, and we just read through, listen, and respond to the questions at the end.
What are the tools in your organisational software toolchain that can assist the DevOps team to identify and prevent data ethical issues?	None that I am aware of in my organisation. We have audit log tools, but I do not know how this works around data ethics. I think for data ethics. Processes can be put in place to ensure ethics but how a software tool can produce such algorithm that can measure, predict, and flag social behaviour is something I find difficult to understand since ethics is about moral obligations.
What strategies do you know that can assist in improving Data ethics within DevOps?	Well, for me, process enforcement is key. There are processes but enforcement is what companies should work on. Maybe this enforcement can be coded so that it is easy to handle and monitor. Also, I think there should be someone nominated from the DevOps team who goes for more trainings strictly dedicated to Data ethics and such individuals can become data ethics champions or evangelist for the DevOps team. This will improve the data ethical practice within the DevOps team since we will have someone close to the team. Currently we have someone in the DevOps team that is the Security evangelist, and this has enhanced the security consciousness in the team. So, like I said, having similar role for data ethics will be a nice idea to introduce in the team.

Table 7. Interview conversation with Participant 2

Participant 2 [P2]	Senior DevOps Engineer/Consultant
Years of Experience within DevOps	5 years
Does your organisation develop solutions for diverse clients across the globe or is it limited to a specific geographical location?	Yes. My main employer and the company I am seconded to have solutions that are used globally and the clients are spread all over.
What does DevOps mean to you and to what extent is it being practiced in the organisation you work with?	DevOps itself is a way of thinking. Some people think it is a title, but it is not. It is like a cultural thing. The way you want to work or the way you want to do things. Before now you would have the developers do their coding on the computer, and once they finish, they just push it away with the mindset that I've done my part, this is it. And then the operations people need to crack their head around it, to get it to work in the environment they want it to work. But when you have a DevOps mindset, that changes completely. Means from the first minute someone is writing the first code on his computer, he's already thinking about how that program is going to be in the actual environment. Maybe he doesn't have this knowledge of writing the pipeline and stuff like that and this is where someone like me comes in. I tell him or her this is the pipe or pipeline you will use to push your code to the repository. This Pipeline is going to see a difference in the commits, and then it's going to start a job that will take this code to a specific environment. And before getting into this environment, it will go through some

	quality assurance, unit test, integration test, compliance test to check for data and configuration compliance. This is where QA comes in. But all of this is happening in the pipeline that the DevOps person needs to write. So, if that makes me a developer as well because I have to develop these pipelines then that means I'm also a developer, only that I am not just developing a software. Instead, I'm developing a pipeline that the software developer is going to use.
What does data ethics mean to you?	For me, I know ethics has to do with what is right and what is wrong, and it differs from one person to another because what is right to me may be wrong to the next person. So, when you bring data into the definition of ethics it means what do you do with data. How do you manipulate data? Are you taking undue advantage of the data you have for whatever benefit. That is my understanding.
What are the business benefits of adherence to ethics of data usage and implications of data ethical breaches?	Yes. Personally, I do but business wise I do not know. I believe every data that is collected by organization is used towards what they want to achieve maybe improve sales. But what the company do further with the data. I don't know. I mean, they can do whatever they want with it as a business but because I'm just a worker and not management, so I don't know.
What are the obstacles to achieving high level of data ethics within the DevOps practice?	Atimes you have not run the data set as you received it but also manipulate it in order to be suitable for the test you are trying to get done as fast as possible. This is data modification without approval or consent. For example, you want to carry out a test on an application or program and you need data set. The current program is developed for APAC region. That is Asia Pacific region but getting data set from the APAC region may be taking too long. Now you decide to use an already existing data set to quickly run your test and you later clear off these data set so as to be able to meet up with deadlines. This is an ethical issue. Though no one is going to know but still you didn't get consent before using this data set. You have breached this data that has been entrusted with you.
Have you found yourself in situations where you needed to compromise on data ethics while attempting to optimize release frequency and velocity?	Yes, I have though it was beyond me. I just found myself doing that because I was told to do that and manage the client's expectation. I had this experience in my previous job. Like, developing a solution for a company in United Kingdom. Their data is not supposed to leave UK but we the developers are in Germany developing the software to manage their need. We were lagging on the project. We needed to do some test and the client sent over to us actual data that was not supposed to leave UK based on regulation. That is because they were under pressure to get the application running as soon as possible. We manipulated the live data sent to us and used it for our own test. So sometimes, pressure is not just even on the DevOps team. It can also be on the actual owner of the data which are the clients, and we care less since they gave the data to us. We just use.
Does your organisation and DevOps team have a staff role dedicated to and accountable for Data Ethics?	There is someone for the organisation, but I think it is about compliance. I am not sure if he also covers issues related to data ethics, privacy, and the rest. Also, this person calls on staff when he observes deviations from laid down procedures. However, there is no one particularly dedicated to this in the DevOps team.

Who is primarily responsible for Data Ethics and Privacy in your organisation.	I do not know. Maybe someone in management.
How does your organisation ensure compliance to Data ethical and privacy laws and regulations for multiple global projects?	There is this part in software development called compliance as code. We have a framework already such that when we are developing, and we enter in the region that we are developing for then it tells us this is what you are permitted to do or not. For example, you are developing a web application for a client in Europe, it is going to immediately add the GDPR framework within the code. Also, in my company there are departments whose main job is to look at the law, that what is allowed in this region and what isn't allowed, but that is in my parent company and not the company I am seconded to. So, data Privacy and Security is part and parcel of compliance as a code. These compliance policies are written as tests. They help my company in detecting and preventing compliance breaches.
Is there a data ethics policy and data governance framework in place in your organisation and are you aware of the content of the policy and the framework?	My organisation follows the GDPR framework though I do not know much about it. For the data ethics policy, I am not sure, but I am aware I was given a security policy document when I joined. Not sure if it covers data ethics as well.
What are the data ethics control and reporting processes in place in your organisation to mitigate against data ethical issues within the DevOps practice?	In my parent organisation, there are some control processes in place. For example, when trying to provision in the cloud environment for clients outside the EU region, some rigorous approvals need to be sought and I am certain these approvals have to do with controls relating to data privacy and local laws of these regions that are outside the EU region which is the primary area of business. For the reporting process, I do not know maybe because I have not found a need to report a breach.
How does your organisation measure and monitor the effectiveness of the controls?	For the measuring and monitoring of the controls I am not aware of such. But there may be these processes in place.
Are there formal data ethics awareness trainings in your organisation for DevOps team and how frequently is it conducted?	Yes. There is Data ethics awareness training in my organisation, and it is a compulsory training. However same training is delivered for every staff of the company and not specifically dedicated for DevOps team.
What are the tools in your organisational software toolchain that can assist the DevOps team to identify and prevent data ethical	None that I am aware of right now. But the compliance as a code tool will flag issues whenever you are developing does not comply with the framework.

issues?	
What strategies do you know that can assist in improving Data ethics within DevOps?	I think the first is training. My organisation has ethics training, and it happens 3 times a year and it is a compulsory and monitored training. Staff are made to realise that their employment can be terminated if they do not undergo the scheduled trainings. Another thing is there should be automated process that helps review compliance. Also, there should be compliance officer that can respond because even if you put controls in place and no one is monitoring then some people will not comply. Also, there should be a defined reporting process, preferably anonymous so that I can mention any ethical issues I find out without any fear of being victimised.

Table 8. Interview conversation with Participant 3

Participant 3 [P3]	IT infrastructure Administrator/Operations
Years of Experience within DevOps	3 years
Does your organisation develop solutions for diverse clients across the globe or is it limited to a specific geographical location?	We have an application used by customers mostly artists, musicians, across the globe for managing their rights and royalties but that doesn't necessarily say that data is sitting across the globe. So, there is a membership portal that the members have access to and there is a centralised backend database also.
What does DevOps mean to you and to what extent is it being practiced in the organisation you work with?	In my company, we have an application team that consist of developers. They are responsible for the development, pushing and debugging of the codes while my team is responsible for the infrastructure side of things. DevOps to me, it just like the structure for the development of applications and the delivery of applications. And how quickly you can deliver the application from when you start writing the code to when the code is deployed and debugged. It also involves the process where you also keep updating the application. So, I believe DevOps encompasses all these things. so that's not like an official definition. That's just like my understanding of it. So, DevOps is about the speed at which organizations deliver applications to their customer. There is a term synonymous with DevOps and we call it CICD. that is continuous integration and continuous development. My organisation practice DevOps at full scale and I am very familiar with DevOps practice.
What does data ethics mean to you?	I just think it's something related to how data is generated, collected, and disseminated in a secure way in order to check the impact of the method of sending, receiving and storing data so that it does not have an adverse impact on data. That's my belief of what ethics is about. I wouldn't come from this position that I understand exactly what data ethics is. It is just my perspective of data ethics as how data is secured, how data is stored and analysed. I have been trained GDPR in my previous company. For GDPR you have all these rules, you have, like

	someone that is responsible for collection. You have different roles assigned to different people. I am not sure if GDPR affects North America region. It looks more at who European data is shared with, how is it collected and analysed.
What are the business benefits of adherence to ethics of data usage and implications of data ethical breaches?	It raises the profile of the company and makes them avoid fines. They also earn the confidence of their customers. For breaches, depending on where the data is stored, you are at the risk of violating something like GDPR which comes with fines. And I know in the last few years, technology companies have been fined. I have worked in the past with a technology company who was under a lot of data ethical scrutiny and pressure.
What are the obstacles to achieving high level of data ethics within the DevOps practice?	Thinking about my own situation, customer biodata and financial information stored in a database can be manipulated by backed staff for malicious reasons especially when those data are in plain text and not masked. Sometimes it's just innocent and not intentional. They may be unaware that they are doing something wrong. They may not know that it is unethical to manipulate a client's data without consent or approval. That is where the need for training and retraining comes into play. Also, the data may be left in a careless way such that unauthorised persons may have access to such information and use it without consent or approval of the client. Reason why we ensure that data and communication is encrypted. Also, where data is kept, who have access to data and how do you keep the data? Are you exposing customer A data to Customer B? Especially now that all customer information is in the same place in cloud which can increase exposure risk.
Have you found yourself in situations where you needed to compromise on data ethics while attempting to optimize release frequency and velocity?	No. None that I am aware of. I won't do that because I understand the implication of such. In my previous company, it was a requirement for all staff to know what GDPR is and sign undertaking after going through the GDPR training. Those guidelines help staff know their boundaries on data handling.
Does your organisation and DevOps team have a staff role dedicated to and accountable for Data Ethics?	No. We are more concerned about security.
Who is primarily responsible for Data Ethics and Privacy in your organisation.	None that I am aware of.
How does your organisation ensure compliance to Data ethical and privacy laws and regulations for multiple global projects?	My organisation does not have multiple global projects but just a solution or an application used by multiple clients. We make customers give approval before we manipulate or make changes to their data, thereby giving them ownership of their data and improving trust.

Is there a data ethics policy and data governance framework in place in your organisation and are you aware of the content of the policy and the framework?	The talks and focus in my company is more on security. There may be some data ethics consideration, but it is not clearly defined or communicated.
What are the data ethics control and reporting processes in place in your organisation to mitigate against data ethical issues within the DevOps practice?	No, none I am aware of. Most big organisations are scared of fines from regulatory bodies, so they put a lot of processes in place to prevent going against government policies and regulations. The organisation I work for is relatively small in size.
How does your organisation measure and monitor the effectiveness of the controls?	None
Are there formal data ethics awareness trainings in your organisation for DevOps team and how frequently is it conducted?	No. There is none. Only security awareness training. I am not sure we have any regulations for data ethics in north America. Based on my previous experience I have asked questions on how we do this and that but no clear answer to my questions from those who are supposed to know. I do not think we have anything like GDPR here in north America. Maybe they have in California in USA.
What are the tools in your organisational software toolchain that can assist the DevOps team to identify and prevent data ethical issues?	We have an audit tool that helps to track who have accessed data. More like a tool for audit trails.
What strategies do you know that can assist in improving Data ethics within DevOps?	I will recommend employee trainings, give more data control to customers, be more transparent on how you handle their data and ensure there is internal policies the DevOps team is aware of and ensure they follow such. Also provide communication channels where team members can report unethical practices.

Table 9. Interview conversation with Participant 4

Participant 4 [P4]	DevOps Engineer/Consultant
Years of Experience within DevOps	2 years
Does your organisation develop solutions for diverse clients across the globe or is it limited to a specific geographical location?	I work in a global consulting firm, and we have clients everywhere. I have three clients assigned to me for now and every client is making use of DevOps in a different way. But in all my task is to reduce the time taken in their processes and this I do through process automation.

What does DevOps mean to you and to what extent is it being practiced in the organisation you work with?	So usually, if you remember, like the beginning of the software development process, it is straightforward you just plan something and try do it as planned. So next came agile that helped to update time to time and improve the program being developed. But still the problem is if developers are doing some tasks, The operations team like the people who are testing, people who are deploying they just seat and do nothing. So now, with the DevOps practice if I have a sprint, which is like 15 days, I develop like a small microservice unlike before when the entire application is just one. So, developer can develop like just a slight or minor improvement in whatever application and just send it to the DevOps team. The DevOps team will take care of the testing, they will create an automation for testing and as soon as possible they deploy it to the client. So that means before when you want to deploy an application, you have to wait the entire cycle but now you do not have to because of the synergy between all teams involved.
What does data ethics mean to you?	For instance, now I got a call from someone, and I have no idea who it is and where they got my mobile number from. So, if someone provides you data about themselves, that is for you alone and do not share or sell their data to others without their permission. That is my perspective. I feel there should be restriction to the extent you can use people's data without their consent.
What are the business benefits of adherence to ethics of data usage and implications of data ethical breaches?	I would say the major business advantage is getting the client's trust. Then this will also increase your client base and of course profit of the business. And vice versa, when there are data ethical breaches, business will lose customer trust, earn lesser revenue, focus less on product development and they will spend more on marketing and adverts in order to earn customer trust.
What are the obstacles to achieving high level of data ethics within the DevOps practice?	99% of the time this is introduced by humans. It is not a technology problem. It could be errors or intentional. The DevOps person may not have been trained properly on how to handle personal data or may even decide to be mischievous despite the trainings. Also, sometimes the pressure to get this done quickly may make the developer or the operations person not to follow laid down procedure. Also, sometimes team members need help from each other and in the process of requesting or receiving help, other members who ideally have not been setup to have access to specific data may end up knowing what they are not supposed to know. Most big organizations however have introduced measures to reduce the likelihood of these data ethics occurrence, but this may not be the case with startup companies.
Have you found yourself in situations where you needed to compromise on data ethics while attempting to optimize release frequency and velocity?	No. Never. I have not done such. The organization provides us with a list of rules we must follow when handling data.

Does your organisation and DevOps team have a staff role dedicated to and accountable for Data Ethics?	Yes, there is a team responsible for that at the organisational level and we have a clear communication channel with the team. We do not have anyone assigned such role in the DevOps team.
Who is primarily responsible for Data Ethics and Privacy in your organisation.	I suppose same team at the organisational level is responsible.
How does your organisation ensure compliance to Data ethical and privacy laws and regulations for multiple global projects?	I can't answer that question. I don't have any answer to that question so far. I honestly do not know. This is a behavioral issue. I am wondering how compliance can be enforced when workers chose to deviate more so it can be difficult to detect.
Is there a data ethics policy and data governance framework in place in your organisation and are you aware of the content of the policy and the framework?	I am not aware of any specific data governance framework being followed. We learn generally about data ethics during awareness training, but I do not have access to any data ethics policy document.
What are the data ethics control and reporting processes in place in your organisation to mitigate against data ethical issues within the DevOps practice?	I do have experience with some of my colleagues who work a lot with data. They don't access the data at all, they just process the data. So, my organization makes sure that there is limited access to the client data, and this reduces the chances of data ethical breaches.
How does your organisation measure and monitor the effectiveness of the controls?	I am not aware of such.
Are there formal data ethics awareness trainings in your organisation for DevOps team and how frequently is it conducted?	Yes. my organisation has trainings dedicated to data ethics, but this is a general training for all staff and not specific to the DevOps team. Also, sometimes for staff there is not enough time to focus on training content, so DevOps staff just keep trying to answer the questions several times just to pass the compulsory assessment and not really with mindset to know the training content.
What are the tools in your organisational software toolchain that can assist the DevOps team to identify and prevent data ethical issues?	No. I am not aware of such.
What strategies do you know that can assist in improving Data ethics within DevOps?	You can train people who make mistakes or errors or do not know about data ethics. But it is difficult to handle data ethical issues for those who intentionally decide to breach data for personal gains. The individual's mentality and intention really matter a lot in data ethics. Mitigating measures can be put in place but there is a limit to how far they can be effective. That is my own opinion.

Table 10. Interview conversation with Participant 5

Participant 5 [P5]	Senior Backend Engineer
Years of Experience within DevOps	4 years
Does your organisation develop solutions for diverse clients across the globe or is it limited to a specific geographical location?	My organization develops software solution for diverse clients across the globe. We are not limited to our local space.
What does DevOps mean to you and to what extent is it being practiced in the organisation you work with?	DevOps is basically the coming together of the development and operations team. Traditionally, these two teams work in silos. When issue arises, it becomes difficult to figure out what went wrong and where it went wrong. The concept of DevOps ensures a synergy between the development team and operations team such that participants involved, kind of have an idea of what occurs in the entire software development lifecycle. Talking about from the point of information gathering to the point of development, point of deployment, to the point of testing and monitoring, and so on, and so forth. So, this eventually kind of bridge the communication gap between development and operations sides of things and with these releases become faster.
What does data ethics mean to you?	So, basically, they are guidelines that govern how customer data are being handled.
What are the business benefits of adherence to ethics of data usage and implications of data ethical breaches?	Primarily, it is trust. So, when your customers are confident that you handle their data with transparency, and you always seek consent, before you do anything with their data. They believe that you follow compliance in handling their data. So, they have this trust in you and stick with you. However, when there are breaches, you lose their confidence, and they doubt if they can actually do business with you. In terms of monetary value, the business loses revenue when they have to use a bunch of their income to pay fines. The company also lose trust of customers and the number of users on the platform will decline because of this trust issues.
What are the obstacles to achieving high level of data ethics within the DevOps practice?	I think primarily is the lack of proper education, I mean training and awareness among members of the DevOps team. For example, here in Nigeria, the government has set up a regulatory body with laws similar to the GDPR in Europe. However, some DevOps team members might not even know that what they are doing is unethical and constitute data breach. These gaps are there always. Also carelessness on the part of the team which is human factor, because the actual process or guidelines of DevOps if properly followed will avoid such occurrence.
Have you found yourself in situations where you needed to compromise on data ethics while attempting to optimize release frequency and velocity?	No. I have not found myself in such situation.

Does your organisation and DevOps team have a staff role dedicated to and accountable for Data Ethics?	Yes, there is a data protection officer in the organisation. There is none within the DevOps team, so he oversees that as well.
Who is primarily responsible for Data Ethics and Privacy in your organisation.	Maybe also the data protection officer. He should be responsible for any issue related to data handling.
How does your organisation ensure compliance to Data ethical and privacy laws and regulations for multiple global projects?	The government of Nigeria have something like the GDPR. This is called NDPR. So, the law mandates that every company that handles client personal data must have a dedicated data protection officer in charge of data and ensure all applicable laws are followed. So that is how data ethics is being managed in my organization.
Is there a data ethics policy and data governance framework in place in your organisation and are you aware of the content of the policy and the framework?	No, I am not aware of any data ethics policy or framework in use.
What are the data ethics control and reporting processes in place in your organisation to mitigate against data ethical issues within the DevOps practice?	Honestly, I do not know the process. I assume all is being handled by the data protection officer, but I am not privy to how it works. For the reporting or communication, I am not clearly aware of it. I think the data officer relates with the senior managers and team leads and I do not know the communication process. The company I worked for before have a huge customer base and they deal with much higher volume of customer personal data. So, they are kind of more concerned about ethical and privacy issues unlike the ones I work with currently. I think the product line matters when it comes to how companies care about this issue.
How does your organisation measure and monitor the effectiveness of the controls?	I do not know.
Are there formal data ethics awareness trainings in your organisation for DevOps team and how frequently is it conducted?	No, we do not have training focused on Data Ethics. What we have regularly is cybersecurity focused trainings.
What are the tools in your organisational software toolchain that can assist the DevOps team to identify and prevent data ethical issues?	None that I can refer to.
What strategies do you know that can assist in improving Data ethics within DevOps?	For me, more awareness training for the DevOps team is important. Also, the duties of the data protection officer should be double-checked by an independent entity to ensure the right thing is done always.

Table 11. Interview conversation with Participant 6

Participant 6 [P6]	Web Developer
Years of Experience within DevOps	5 years
Does your organisation develop solutions for diverse clients across the globe or is it limited to a specific geographical location?	Mainly the company product follows a SaaS model and there is nothing practically limiting it to be used by only one type of people from the business side. The main target audience is Europe and there are more users of the solution in Europe. But there is still a strong connection with the product from Asia, South America and African. It serves different geographical location.
What does DevOps mean to you and to what extent is it being practiced in the organisation you work with?	I think two units are working in harmony in a nice way that there isn't like a big obstacle or like any in a part of those team are having like a long time doing nothing waiting for the other parts to do something Like the integration, the delivery and the development are working in a nice and smooth way, and it happens regularly and not once in a while. So, the DevOps is mainly the spiral work between those two units and when the Dev team have something to deliver the Ops pick it and take care of deployment and ensure the developed solution is delivered to the end user. In our case, the teams are totally distinguishable but still there is strong collaboration in the manner of work.
What does data ethics mean to you?	I have heard about it but I am not experienced there. The first thing that came to my mind when I hear data ethics is related to big data and what you are doing with it. Basically, how companies and enterprises around the world are handling and managing the data that are gathered from the users. I think they said that most of the companies right now are more like data companies, so they have a lot of information about the user. So, data ethics is how you manage those data and what level of transparency you have with the data.
What are the business benefits of adherence to ethics of data usage and implications of data ethical breaches?	Yeah. I think one big benefit is building trust with the client, I mean the end user. Not everyone is aware of privacy and data security and ethics. As long as you let them know you are taking care of the data you get from them then you get more trust from the user. They keep buying and using your service. However, if they find out that you are not using the data in the manner acceptable to them, then you can start losing clients and customers. I am not sure if there are other benefits or implications.
What are the obstacles to achieving high level of data ethics within the DevOps practice?	Data ethics could be ignored or omitted during the DevOps cycle especially when DevOps cycle is running fast. Because sometimes I think there is no clear framework, holistic tools, or control to ensure that privacy is taken into consideration. The DevOps team end up caring only about the quality of the code without caring much about ethics related to the data being generated or processed. As Developers we do not usually think much about data ethics. We care more about security and getting the code to work.

Have you found yourself in situations where you needed to compromise on data ethics while attempting to optimize release frequency and velocity?	I have not been in that situation. But it is possible to be in that situation.
Does your organisation and DevOps team have a staff role dedicated to and accountable for Data Ethics?	I am not aware of any dedicated role for such in the organisation or the DevOps team
Who is primarily responsible for Data Ethics and Privacy in your organisation.	I think more of the product owner, and the QA. Though none of them have been formally communicated to me as being responsible for such. It is just my own opinion.
How does your organisation ensure compliance to Data ethical and privacy laws and regulations for multiple global projects?	I think at least for Europe the company have a tool for GDPR. The tool gives the client or the user the option of deleting his data by himself if he doesn't want the data to be in your custody any longer. For the global projects, I am not sure if there are some ISO certificate, they have that ensures data ethics.
Is there a data ethics policy and data governance framework in place in your organisation and are you aware of the content of the policy and the framework?	No. I have not come across any data ethics or privacy policy.
What are the data ethics control and reporting processes in place in your organisation to mitigate against data ethical issues within the DevOps practice?	Actually, I am not aware of any of these internal control processes within the DevOps team, but we have in house QA and some outside consultants who may be responsible for things like this.
How does your organisation measure and monitor the effectiveness of the controls?	I do not know if these activities are conducted.
Are there formal data ethics awareness trainings in your organisation for DevOps team and how frequently is it conducted?	I am quite new in the company. This is my second month. I have not undergone such training. Maybe it is scheduled for later dates. But in my previous company as well no such training was organized.
What are the tools in your organisational software toolchain that can assist the DevOps team to identify and prevent data ethical issues?	I also do not know of any tool that can assist the DevOps team to identify data ethical issues within except the tools that allows clients to delete or handle their personal data remotely.
What strategies do you know that can assist in improving Data ethics within DevOps?	I think the main thing to do is share a lot of awareness about Data ethics because it is a big umbrella under where lots of things are to know about.