A Semi-Formal Specification Language Approach for Security And Privacy Compliance for SaaS Business Applications – Nigerian Privacy And Data Protection Regulation as a Case Study

by

Hammajam Ahmed Adamu

A thesis submitted in partial fulfilment for the requirements for the degree of Doctor of Philosophy at the University of Central Lancashire

1828

University of Central Lancashire

UCLan

November, 2021

Declaration

STUDENT DECLARATION FORM

Type of Award:	**Doctor of Philosophy**
School:	**School of Psychology and Computing**

1. Concurrent registration for two or more academic awards

I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the University or other academic or professional institution.

2. Material submitted for another award

I declare that no material contained in the thesis has been used in any other submission for an academic award and is solely my own work

3. Use of a Proof-reader

The following third party proof-reading service was used for this thesis - *A Semi-Formal Specification Language Approach for Security And Privacy Compliance for SaaS Business Applications – Nigerian Privacy And Data Protection Regulation as a Case Study* in accordance with the Policy on Proof-reading for Research Degree Programmes and the Research Element of Professional Doctorate Programmes.

A copy of the confirmatory statement of acceptance from that service has been lodged with the Research Student Registry.

Signature of Candidate:

Print name: Hammajam Ahmed Adamu

Proofreading Declaration

uclan
University of Central Lancashire

Declaration of Proof reading Services

Confirmatory Statement of Acceptance

Name of Candidate	**Hammajam Ahmed Adamu**
Type of Award	**Doctor of Philosophy**

I declare that I have read, understood and have adhered to UCLan's Proofreading Policy (Appendix 1) when proof reading the above candidate's research degree thesis.

Name of Company: Proofedreadmyessay.co.uk

Contact Details:

Telephone: +4402032397323

Email: info@preefreadmyessay.co.uk

Abstract

Software as a service (SaaS) is described as a situation where a full application is managed and hosted by the service provider with users or customers consuming it over an internet connection using a web browser. SaaS applications have a wide range of use cases and benefits and have continued to become increasingly important across all sectors where security, privacy, and data protection are fundamental.

Furthermore, the need for compliance with data protection regulations in SaaS applications has increasingly received attention, with governments coming up with regulations such as the European Union General data protection regulation (GDPR 2018) and the Nigerian data protection regulation (NDPR 2019) to ensure adequate protection, particularly personal data.

To date, some existing works have covered data protection compliance efforts that relate to the GDPR. Therefore, given the limitations of the existing approaches, there are none dedicated to helping organisations comply with the NDPR data protection requirements regarding personal data. Nevertheless, there are many similarities between the two sets of regulations, so looking at the GDPR literature means that it is still possible to study the NDPR and Nigerian organisations’ compliance efforts.

In this thesis, the above concerns are addressed through the execution of a design science and semi-formal methods to investigate, translate and map the legal compliance requirements of the NDPR data protection properties, and aligning them to the data life cycle for ease of encoding and specification of the compliance check procedure within the context of SaaS applications.

Additionally, this is in tandem with the principles of Privacy by Design (PbD) principles. Secondly, based on the translated and mapped requirements, the security, privacy and data protection requirements were condensed to make them applicable to the context of SaaS applications and to express them using an extended semi-formal policy language variant of the PrimeLife policy language (PPL) called the SaaS-PPL. Thirdly, the extended policy language, SaaS-PPL, is then used to model a compliance check syntax and show proof of compliance when all properties are matched to validate and show the policy language's applicability within the context of SaaS applications.

Finally, the extended policy language, SaaS-PPL, is evaluated in an NDPR case study within a retail scenario such as a smart retail pay-at-the-pump showing how compliance to NDPR's security, privacy and data protection properties is achieved when personal data is collected, processed, retained, stored and shared. Upon applying the SaaS-PPL policy language to express the NDPR requirements, the online platform shall become compliant with the NDPR based on the semi-formal proofs properties.

Table of Contents

Acknowledgement

I thank Allahu *azza wa jalla,* who made it possible for me to see this day alive and in good health at an unprecedented time during the COVID-19 pandemic. My special gratitude goes to my parents, who have, against all odds, supported me throughout my life and educational journey. May Allah reward them abundantly.

I also sincerely thank the Executive secretary and management of the Petroleum Technology Development Fund (PTDF), particularly the GM Training, Tijjani Ahmad Galadima.

I am particularly grateful to my supervisor, Dr Mahmud Hashem Eiza, for the leadership, guidance and for being there from the early days of my research to this day. Dr Max has been patient, kind and indeed very supportive with his invaluable feedbacks all through. I remain thankful and appreciative from the depth of my heart. I am also very grateful to Dr Vinh T. Ta, my second supervisor, who provided me with guidance in many ways too numerous to mention. Thank you, Dr Vinh.

I am also sincerely grateful to my panel of examiners Dr Paul Stephens and Dr Josephina Antoniou, for the appraisal.

I am also sincerely thankful to Dr Daniel Fitton, who has, in many ways, provided leadership to the entire team and helped me through every turbulence. Thank you once again, Dr Dan.

I also appreciate the support of my wife, Rashida D. Hammajam, my four children, Maryam, Asma, Dahiru and Adamu, for their love and patience with me throughout this journey. I thank Hon. Awwal D. Tukur, Richards Daniel Laushi and Professor Liman Tukur for the mentoring and support to undertake this giant leap.

I will also like to appreciate the management of NNPC, the DG, NITDA, NCDMB and other vital agencies of the Federal Government of Nigeria who supported this research study and my CM222 lab colleagues, Essa Anas, Wilbert Sinzara, Peter, Omoseye Abayomi Adeyemi and Sanchit Balasaheb Chandile and Abdullah. It has been an outstanding experience sharing the same working space with all of you before the COVID-19 pandemic struck.

List of Tables and Figures

List of Symbols

Symbols	*Meaning*
$\in$	*is an element of*
$\leq$	*Less (or equally) permissive*
$\subseteq$	*a subset of*
$typeset$	*Data type*
Pol	*Service provider policy*
$Pcol$	*Service provider data sub-policy*
$Pproc$	*Service provider data Processing sub-policy*
$Pstr$	*Service provider data Storage sub-policy*
$Pret$	*Service provider data Retention sub-policy*
Pfw	*Service provider data Forwarding sub-policy*
$Pol\_typeset.Pcol$	*Collection policy for types in typeset*
$Pol\_typeset.Pproc$	*Processing policy for types in typeset*
$Pol\_typeset.Pstr$	*Storage policy for types in typeset*
$Pol\_typeset.Pret$	*Retention policy for types in typeset*
$Pol\_typeset.Pfw$	*Forwarding policy for types in typeset*
REQ	*User preferences*
$R\_typeset1$	*User preference types*
$Rcol$	*User preferences on data Collection obligations of a service provider*
$Rproc$	*User preferences on data Processing obligations of a service provider*
$Rstr$	*User preferences on data Storage obligations of a service provider*
$Rret$	*User preferences on data Retention obligations of a service provider*
Rfw	*User preferences on data Forwarding obligations of a service provider*
$(cons)$	*Element for consent collection*
$(cpurp)$	*Element for data collection purpose*
$(procpurp)$	*Element for data processing purpose*

$whocanproc$	*Element for who can process data*
$notify$	*Element which captures notification before or after data processing*
$wherestore$	*Element preferred set of places where data is stored*
$howstore$	*Element for method of how data is stored i.e. encrypted or available*
$fwpurp$	*Element for purpose of data forwarding*
$3rdparty$	*Element for list of third-party recipients of data*
$placeret$	*A set of elements describing location of data retention*
$when$	*Element describing when data is retained*
$rdelay = dd$	*Numerical retention value for data retention delay*
$gdelay = gd$	*Numerical retention value for data retention at global level*
$decl$	*Element for declaration i.e. Y or N*
$SPstorage$	*Element for Service provider storage*
$mainstorage$	*Element for main storage location for data retention*
$backupstorage$	*Element for backup storage location for data retention*
$time - tvalue$	*Minus operation*
$SpOwnServer$	*Element for service provider's storage infrastructure*
$spkey$	*Element for service provider key*
$Hidden$	*Encrypted and not available to service provider*
$3rdPartyServers$	*Third-party storage servers*
$AvailSpOwnServerable$	*Encrypted and available to service provider*
$Clientplace$	*Element for client or user storage location.*
$Pol \leq REQ$	*Where service provider policy is less than or equal to the user preference(s)*
$Pol\_typeset\_i$	*Service provider policy element*

CHAPTER ONE

1.0 Introduction

Recent advances in the ways in which services can be delivered over the Internet have unlocked significant opportunities for software companies (Chen, H. 2016) and accelerated new service platforms such as Software as a Service (SaaS) applications. However, they have also generated problems for example personal data privacy and protection issues, leading to fears that people's fundamental rights and personal data will be abused.

One way to address these challenges is to ensure compliance with data protection regulations and to apply relevant concepts such as Privacy by Design, championed by Anne (Cavoukian 2008). To contribute to solving the growing data protection challenges faced by users and organisations alike, Cavukian has advanced seven Privacy by Design principles in order to include means of enhancing privacy and data protection mechanisms for example in SaaS applications platforms and technologies at the development level.

Although, many efforts have been launched to give citizens and individuals data protection rights whenever their data are processed, whether in physical or digital format. In 1981, the Council of Europe issued a convention with the intention of protecting personal data. This convention extended numerous rights to citizens of EU countries, while Directive 95/46 / EC conferred additional rights to all EU peoples (A. S. Ahmadian, J. Jürjens 2016). In April 2016, the European Parliament agreed on the new General Data Protection Regulation (GDPR); this entered into force in May 2018 (L. Elluri, A. Nagar et al. 2018a), with jurisdiction across the entire European Union.

The GDPR for example, introduced, several novelties to personal data regulation such as Article 25, which requires privacy mechanisms to be included in designs by default. Other requirements of the GDPR include a right to erasure, consent to data collection before processing, transfer personal data to another data controller, and be notified of any personal data breach within 72 hours. Data protection agencies have been established to implement these provisions, such as the Information Commissioner’s Office (ICO, 2019c) in the UK.

In countries around the World, a handful of data protection regulations have been implemented. For example, the Nigerian Data Protection Regulation (NITDA 2019) in Nigeria, which was set up in 2019, following in the footsteps of the GDPR (Brodin 2019a).

1.1 Research challenge

Legislations aimed at data privacy and protection such as the NDPR and GDPR require all public data-processing organisations to comply with these regulations. The level of compliance has been significantly increased by raising awareness among citizens about their data protection rights, while imposing compliance restrictions on data controllers and processors. Implementing mechanisms to guarantee security, privacy and personal data protection in any system for instance, SaaS applications is a significant challenge. Organisations that collect personal data must abide by privacy, data protection, and security provisions and failure to do so under the GDPR will result in the imposition of penalties to the tune of 4 per cent of their yearly revenue or a penalty of up to EUR 20 million. The equivalent figure for the NDPR is 2 per cent of annual gross revenue for data processors that manage the data of at least 10,000 users or data subjects and 1 per cent for data processors with less than 10,000 data subjects.

Researchers have investigated the issue of how to ensure that IT infrastructures and systems such as SaaS applications comply with privacy and data protection regulations. However, while there exist various works which have covered compliance efforts that relate to the GDPR, there are none dedicated to helping organisations comply with the NDPR data protection requirements. Nevertheless, there are many similarities between the two sets of regulations, so looking at the GDPR literature means it is still possible to study the NDPR and Nigerian organisations' compliance efforts.

1.2 Motivation

Currently, there is significant interest in enforcing compliance with data protection regulation relating to privacy and security of personal data in SaaS applications from industries in Nigeria such as the retail sector, because of the potential benefits SaaS applications could bring to the industry. However, the Nigerian data protection regulation NDPR aimed at ensuring the protection of data owners' privacy and rights is a legal textual document and therefore unable to ensure compliance. Thus, achieving compliance with data protection such as the NDPR is critical to the continued adoption of SaaS in Nigeria in a retail context.

Therefore, the following form the bases of this thesis findings and contributions to privacy and data protection compliance: a) the exploration of the critical compliance challenges faced by organisations desirous of using SaaS applications and generally cloud computing solutions. b) the advancement of a means of achieving compliance with data protection regulations with a focus on SaaS applications to organisations desirous of complying and moving away from textual compliance by embedding privacy and data protection compliance in their processes, systems, and technologies. c) applying a language-based compliance technique to relevant examples or use cases based on the NDPR data protection regulation.

Additionally, the researcher was motivated to learn more about SaaS applications and cloud computing, particularly privacy security and data protection and making valuable contributions, mastering relevant skills, recognizing the inherent limitations of these skills, and communicating outcomes professionally.

Solving these key challenges have motivated this research exercise, which has given rise to a novel means of compliance with data protection regulations with a focus on SaaS applications, one of the three models of cloud computing by organisations who have adopted or implemented SaaS applications to boost their operations and the researcher assumes that SaaS application service providers provide services to customers across a range of sectors and to help organisations achieve compliance with data protection regulations and privacy protocols within the framework of SaaS implementations.

The National Institute of Standards and Technology (National Institute of Standard and Technology -USA 2011) describes SaaS applications as the phenomenon whereby service providers host and administer entire applications, while users and customers use these applications over an Internet connection using a web browser (A. S. Ahmadian, J. Jürjens 2016). The SaaS model is one of the main models of the cloud, with the other two being Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (CSA 2017). A few examples of some sub-models of the cloud that usually depend on any of these three main models include the Function as a Service (FaaS) (B. Li, Z. Li et al. 2021)**,** Data as a Service (DaaS) (Terzo, Ruiu et al. 2013)**,** Container as a Service (CaaS) (Hussein, Mousa et al. 2019) These models depend on the cloud computing paradigm, as they rely on pervasive, on-demand network access to computing resources, usually shared, configurable and capable of being provisioned in a rapid fashion as well as released when not needed with very little effort and little input from the service provider (Tiwari, Joshi 2014a).

Due to the architecture and flexibility that SaaS applications offer organisations, this phenomenon has seen an explosion in interest, with revenue reaching $94 billion in 2019 and expected to revenue to reach $143.7 billion in 2022 (Gartner Inc 2019). SaaS applications provide a number of key benefits to consumers: ease of deployment, pay as you go, pricing models, scalability, and least cost of maintenance. Other benefits include accessibility via the Internet anywhere, anyplace, and at any time, with significant resource utilisation and centralised management also made possible due to multi-tenancy and virtualisation technologies, in addition to the continuous availability that is usually guaranteed by the service provider(Qualtrics 2017). For example, Kongsberg Digital, a solutions provider, provided Shell with a SaaS-based software solution that spans the company's upstream, integrated gas, downstream, and production business lines. Shell gained benefits and capabilities from the solution, including the ability to integrate assets, deliver high-end visualisations, and analytical capabilities on a global scale (Perrons, Hems 2013, Offshore Engineer 2020).

Additionally, the SaaS platform enabled Shell to combine and interpret real-time sensor data from IoT devices, historical data, engineering data, and other transactional business data from a variety of data sources, enabling Shell to digitally improve work processes and maximise facility efficiency.

However, despite these benefits, SaaS applications still suffer from several significant drawbacks (L. Elluri, et al. 2018a) in connection with concerns relating to security, privacy and data protection, for example, compliance, governance control, trust, identity and access management, and incident response issues (NIST-USA, 2011, Di Iorio, Carinci et al. 2020), which have led to more breaches to privacy and security of data in recent years. For example, on one occasion, data belonging to customers of the British Airways Avios software platform were breached due to multifactor-authentication problems on at least 13 critical SaaS applications, according to the ICO's office, which another serious breach affected Marriott International Inc. Under the GDPR, these two incidents attracted fines of £183.39 and £99 million, respectively (ICO, 2019a) In Nigeria, the NITDA recently investigated the activities of Truecaller for the alleged violation of Nigerians' privacy rights (Truecaller 2020). As a consequence of these breaches, organisations continue to face the problem of how to design or align their internal processes and operations with complying with data protection regulations while simultaneously discharging their services without breaching the privacy rights of their customers. These problems become more apparent when organisations adopt or migrate their software assets to the SaaS applications model.

As mentioned previously, managing users' personal data is a major concern in SaaS applications (Wang 2011a). Similarly, in cloud-computing architectures that consist of third-party resources, privacy can be violated by inappropriately implemented privacy settings since users' data are exchanged across multiple business partnerships.

Another matter is that these regulations are usually textual and made up of many legal provisions, making it challenging to ensure the compliance of organisations such as SaaS applications service providers.

Researchers have explored a range of approaches designed to support organisations to achieve compliance with data protection regulations. These approaches and solutions include manual audits, industry certifications, propriety mechanisms, frameworks, architectures, and policy languages such as Primelife (Azraoui, Elkhiyaoui et al. 2015a)—an enhanced XACML access authorisation policy language designed to protect, track access control and authorisations to resources in compliance with the privacy requirements enshrined in data protection regulations. For example, (Jayasinghe, Lee et al. 2018) proposed a GDPR trust-based compliant framework for data controllers, but currently no efforts have been made to help SaaS applications providers to comply with NDPR data protection regulation requirements.

This background offers a solid justification to ensure that service providers in Nigeria abide by NDPR regulations. They can contribute to operationalising compliance with NDPR data protection regulations in SaaS applications by making use of semi-formal methods to design a semi-formal policy language for the specification and reasoning of the data protection properties of the NDPR on an end-to-end basis. The application of the concept of the data life cycle is a requirement within the SaaS context. This concept involves the specification of compliance and data protection properties at the stages of data collection, processing or usage, storage, retention or deletion, and forwarding, where data are forwarded to a third party.

1.2.1 Research questions

The following research questions are proposed here:

1. RQ1. What are the legal requirements of the NDPR, as they relate to the principles of Privacy by Design?

2. RQ2. Can the legal requirements of the NDPR be mapped and aligned to the data life cycle?
3. RQ3. How can privacy and data protection requirements be presented in a semi-formal policy language?
4. RQ4. How can a model of the compliance check syntax show proof of compliance when all properties are matched and validated within the context of SaaS applications?

1.3 About this thesis

This thesis seeks to specify and reason about data protection requirements and properties at the granular level of the data life cycle within SaaS applications by utilising semi-formal methods and techniques to design a policy language made up of syntax and semantics. This being so, specific issues or concerns such as governance, trust issues, and incidence response are out of the scope of this thesis.

The overall aim of this thesis is to design an extended, semi-formal policy language approach to privacy and data protection compliance for SaaS business applications by expressing requirements for a) the privacy of personal data and b) the achievement of compliance with data protection regulations that relate to the privacy of personal data.

1.3.1 Research objectives

To further achieve the aims of this research, the following objectives have been set out:

i) To carry out SaaS focused and NDPR compliance approach research with emphasis on achieving compliance with data protection regulations such as the NDPR in the areas of privacy of personal data, data security, location, multi-tenancy, usage, storage and data forwarding.

ii) To define compliance properties and map the privacy and data protection properties of the NDPR regulation, while aligning them to the data life cycle for ease of encoding and specification of the compliance check procedure, within the context of SaaS applications.

iii)To condense data protection regulation requirements to make them applicable to the context of SaaS applications and to present them as a semi-formal policy language.

iv) To propose a model compliance check syntax and show evidence of compliance when all properties are matched to validate and show the policy language’s applicability within SaaS applications and to evaluate the SaaS-PPL within an NDPR as a case study in a retail context.

Achieving the first objective (i) is the first step in addressing the research challenge and could, perhaps, trigger subsequent research to further understand the challenges and propose newer alternatives solutions. The achievement of the second objective (ii) will have a two-fold benefit: a) to define and map compliance properties to address the problem of the privacy of personal data and b) to align these properties to the NDPR regulations for ease of encoding and specification. The third objective (iii) is set out for two purposes: a) to convert the applicable data regulations requirements to the context of SaaS applications and b) to present these requirements within the syntax and semantics of a semi-formal policy language. The fourth objective (iv) is to provide a model syntax for compliance check to show proof of compliance when all properties are matched within the context of SaaS applications.

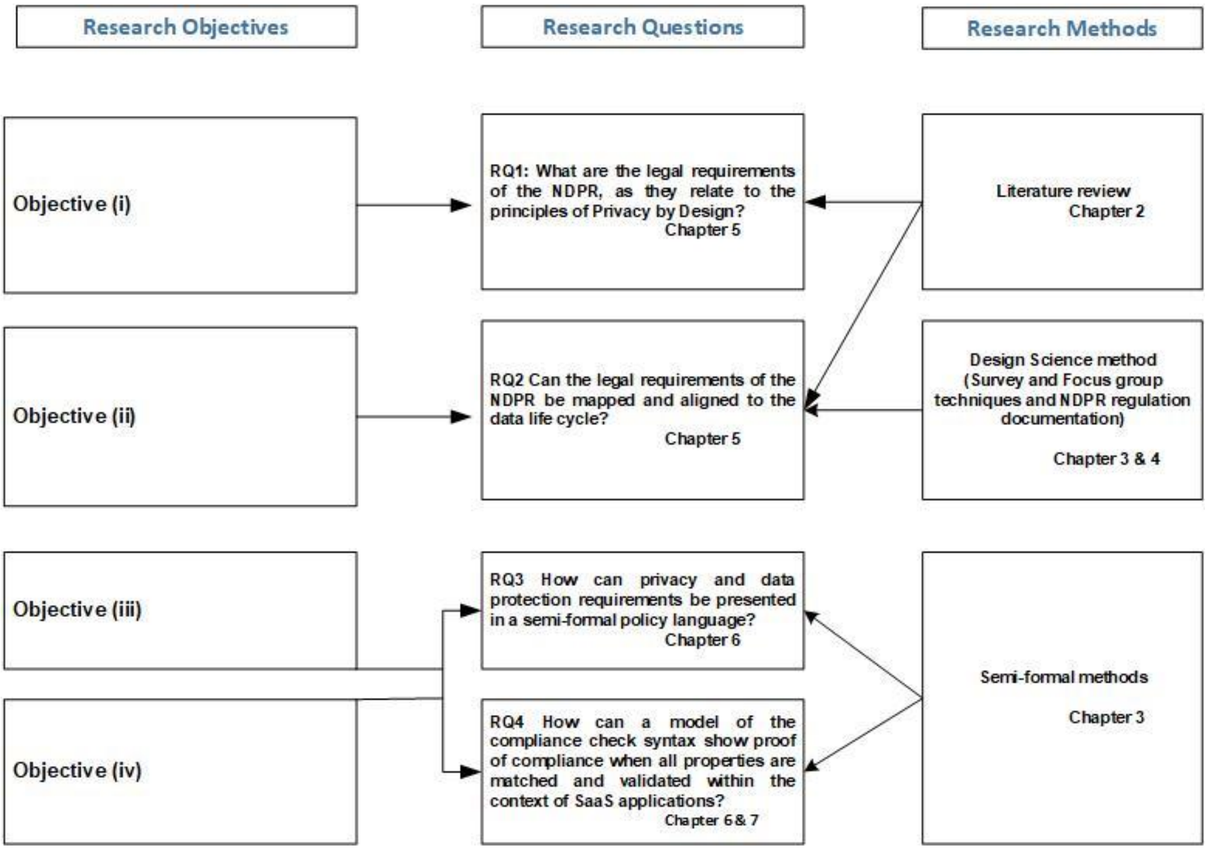

Research Objectives
Research Questions
Research Methods
Objective (i)
RQ1: What are the legal requirements of the NDPR, as they relate to the principles of Privacy by Design? Chapter 5
Literature review Chapter 2
Objective (ii)
RQ2 Can the legal requirements of the NDPR be mapped and aligned to the data life cycle? Chapter 5
Design Science method (Survey and Focus group techniques and NDPR regulation documentation) Chapter 3 & 4
Objective (iii)
RQ3 How can privacy and data protection requirements be presented in a semi-formal policy language? Chapter 6
Objective (iv)
RQ4 How can a model of the compliance check syntax show proof of compliance when all properties are matched and validated within the context of SaaS applications? Chapter 6 & 7
Semi-formal methods Chapter 3

Figure 1: Research objectives, questions and methods mapping

1.3.2 Contributions

1. SaaS and NDPR focused compliance approach/mechanism

The first contribution is a SaaS focused and NDPR compliance approach with an emphasis on achieving compliance with data protection regulations such as the NDPR in the areas of privacy of data, security, location, multi-tenancy, usage, storage and data forwarding within the context of SaaS applications. The focus on SaaS applications resulted in new knowledge that may be used as an initial benchmark for policy language extensions and that should be considered when proposing extensions for implementing the language in different scenarios such as in an on-premises SaaS scenario.

2. Mapping the privacy and data protection properties of the NDPR

The second contribution is to map the security and privacy provisions of the NDPR regulations and align them to the data life cycle for ease of encoding and specification. SaaS application service providers collect users' data to enable their applications or services, thus creating the need for bodies to ensure compliance with data handling regulations. This research considers a scenario in which data are collected and transferred out of the data subjects' control to the service provider's infrastructure. The data could be used in ways that conflict with the data subjects' data handling preferences, thus raising privacy and data protection concerns over a potential loss of control over personal data (Trapero, Modic et al. 2017).

In order to deliver this contribution and alleviate these concerns, an analysis of the obligations of data controllers as detailed in the NDPR is carried out, and a policy language presented to articulate the data-handling rules that correspond to data collection, usage, storage, deletion and retention, and forwarding.

3. Development of a Syntax and semantics of the SaaS-PPL

The third contribution is the conversion of the data protection regulation requirements in a condensed way that is applicable to the context of SaaS applications and presented as a semi-formal policy language. This was done by keeping the fundamental roles defined in PrimeLife policy language, access control and authorisation policy language (Slim Trabelsi , Akram Njeh , Laurent Bussard , Gregory Neven 2010). A syntax is presented to specify and express the data protection properties of the NDPR, while the syntax for the policy language policies is defined and aligned to the data life cycle.

4. **Compliance check syntax showing proof of compliance**

The fourth contribution is the compliance check syntax to show proof of compliance when all properties are matched and the validity and applicability of SaaS-PPL in the context of SaaS applications. The compliance check syntax is designed to show proof of conformance when a service provider's preferences are matched with the data subjects' preferences.

1.4 Research methods and approach

The aim of this research work is to design an artefact, therefore, the researcher employed the design science and semi-formal methods as put forward in (Brodin 2019a, Li, Werner et al. 2019, Russell, O'Raghallaigh et al. 2018), which are excellent choices for the research context. In design science, the built artefact can be a model, process, method, or design in theory (Russell, O'Raghallaigh et al. 2018). Design science deals with two challenges: how to solve a functional problem in a particular organisational context and to create and validate an artefact—in this case, a way of specifying compliance requirements that pertain to the recognised problem such as compliance with novel data protection laws; and how to technically design something that requires a problem to be first identified in practice (Li, Werner et al. 2020), (Serrado, Pereira et al. 2020).

Additionally, the researcher collected qualitative data in the early stages of the research using qualitative techniques such as a survey and a focus group session of a select number of high-profile organisations in Nigeria in order to understand the security and privacy concerns of these organisations relating to SaaS applications. These concerns were collected and aligned with the legal requirements from the NDPR, based on the principles of Privacy by Design (A. Cavoukian 2020).

Further, on semi-formal methods, Bjorn et al. (Bj\orner, Havelund 2014) identified semi-formal methods—a methodology whose procedures, tools, and techniques can be described in mathematics. Bjorn et al. described a method of presenting a language to specify requirements, a semi-formal syntax, a structure for the statements, and semi-formal semantics that provides explanations for the logic and meanings of the syntax statements, as well as a semi-formal proof system to prove or disprove the correctness of intended systems or designs. Semi-formal approaches and methods are used to ensure the correct specification and analysis of a specification and subsequently transform the constructed specification(s) into the working system(s) or software. In addition to the construction of specification languages, semi-formal methods are used to construct software packages and solutions.

NDPR (2019) case study

Many organisations in Nigeria, including those that provide SaaS applications, products, and services, are aware that in January 2019, the NDPR legislation established a new framework that regulated how to process personal data. Despite this, many organisations have not effectively implemented compliance processes, are concerned that they are not currently compliant with this legislation and are worried about possible penalties. This being so, these organisations must review their processes, ascertain what data they collect, how they utilise it, and, ultimately, share and transfer data with their third-party partners. In the context of this research, ‘personal data’ refers to knowledge or information regarding a natural being and their personal data, which almost all organisations collect in Nigeria, especially service providers.

One crucial aspect of the NDPR is that it states that an organisation must minimise the personal data it receives and publicise the data collection's intent, making it mandatory for all data controllers to reveal why they are collecting personal data. Organisations and service providers must have a lawful basis for processing personal data and the NDPR has established a variety of lawful bases for various forms of personal data collection. Nevertheless, each service provider must clarify the legal foundation they follow for all the data they collect and process.

It is against the background of these concepts that this research study develops a policy language to capture the properties of NDPR legal specifications to ensure compliance with the NDPR; the case study followed here has been proposed to study how to achieve privacy data protection, and security in SaaS applications.

For example, suppose a service provider is dependent on consent as the legal justification for its gathering of personal data. In that case, it must be willing to show that each individual who has given consent did so voluntarily, that the consent was conscious, and that it was unambiguous. Users must also be given opt-out or opt-in options. This is a significant problem since the NDPR is a textual document, which makes it challenging to ascertain compliance to this basis.

1.5 Thesis outline

The rest of this thesis is structured as follows. Chapter 2 presents a review of the fundamentals of SaaS applications, as they are related to the aim of this thesis. At the same time, it also highlights the concepts of privacy, data protection regulation issues, and compliance and establishes a link between SaaS applications, privacy, and data protection. Chapter 3 discusses the research methodology, including the overall approach taken. Chapter 4 presents the requirements for the

SaaS-PPL policy language and then maps out the obligations of data controllers, as set out in the NDPR regulations that pertain to the need to specify and express policy requirements at the granular level, based on the concept of Privacy by Design, Chapter 5 discusses and presents the results from the data collection and analysis. Chapter 6 presents a novel policy language extension, syntax, semantics, and compliance check semantics and procedures. Chapter 7 uses a case study to show data flows in a scenario showing how data are handled across the stages of a data life cycle within the context of SaaS applications. Finally, Chapter 8 concludes the thesis and discusses some ideas for future work.

1.6 Chapter summary

This chapter has provided a general overview of the thesis. It has highlighted the research context, which is the security, privacy, and safety of personal data alongside compliance challenges with data protection regulations, within SaaS applications. The chapter has also discussed the research challenge, motivation, aims, and objectives, formulated the research questions, outlined the contributions, and presented an overview of the research methods that bind the research process. Finally, the chapter has presented an outline and summary of the thesis as a whole.

CHAPTER TWO

2.0 Related Work

Based on the research objectives and approaches discussed in **Chapter 1**, these areas have been identified as relevant for a review to put the research within context. The review aims to answer questions about SaaS applications, security, privacy issues, and personal data protection, including the PbD concept. Furthermore, the review explores issues with existing approaches to ensure data protection using law and regulation instruments in SaaS applications. These questions and issues are centred around SaaS applications' fundamentals and the concepts of personal data, security, privacy, and data protection. Furthermore, the principle of privacy by design is further reviewed to understand how it can help implement and achieve privacy within the research context.

What is the link between SaaS applications, data privacy, and current data protection regulations, including the issues relevant to this research? Additionally, is there a way to execute data protection in SaaS applications by relying on principles such as privacy by design? Currently, are there methods or approaches to ensure data protection regulation compliance and privacy by design within the context of SaaS applications?

Because the Nigerian Data Protection Regulation (NDPR) is a new regulation that came into effect in April 2019, not enough literature exists on how compliance is tackled, especially concerning security, privacy, data protection, and privacy principles by design relating to SaaS applications and the NDPR. To achieve the review objective, the researcher gathered resources from a wide range of sources, such as academic databases (e.g. ACM, IEEE, Wiley, Gartner, and Springer journals) and relevant data protection regulation documentation such as the NDPR and General Data Protection Regulation (GDPR) (e.g. industry reports and resources such as the CSA Security Guidance). Finally, to construct this thesis’s review section, the researcher followed Randolf and Justus's methods (Randolph 2009).

2.1 SaaS Business Applications– The Fundamentals

The National Institute of Standards and Technology – USA (2011) has described a SaaS application as a situation where the provider manages and hosts a full application, with users consuming it over an internet connection using a web browser. Furthermore, there are three models within the cloud computing system, of which the SaaS model is one. Other models include Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) (CSA 2017). They all rely on ‘ubiquitous, convenient, on-demand network access to a shared pool of computing resources that are configurable, for example, networks, servers, storage, applications, and services that can be provisioned and released with minimal service provider interaction (CSA,2017). Users of SaaS applications are not responsible for controlling infrastructure components such as servers, networks, and, in some cases, application capabilities – except in some user-specific settings.

SaaS applications provide several key benefits to consumers, such as ease of deployment, a unique service payment model requiring users to pay for when a service is used (sometimes referred to as ‘pay as you go’), the capability to scale as usage grows, and least cost of maintenance (Qualtrics 2017). Additional benefits include being accessible via the internet from anywhere, anyplace, and at any time, with significant resource use and centralised management due to multi-tenancy and virtualisation technologies and continuous availability guaranteed by the service provider (Kulkarni, 2013).

SaaS users fall into two categories: everyday users and enterprises or organisations that procure licences and obtain access from SaaS service providers. These users rely on their administrators to configure their SaaS access and settings. Additionally, SaaS applications rely on configurable and multi-tenant architectures that allow users to use their dedicated part of the application – usually on the same hardware. The SaaS architecture is comparable to a service-oriented architecture, where client requests are met even at peak hours and transactions can be processed in a secure and reliable setting.

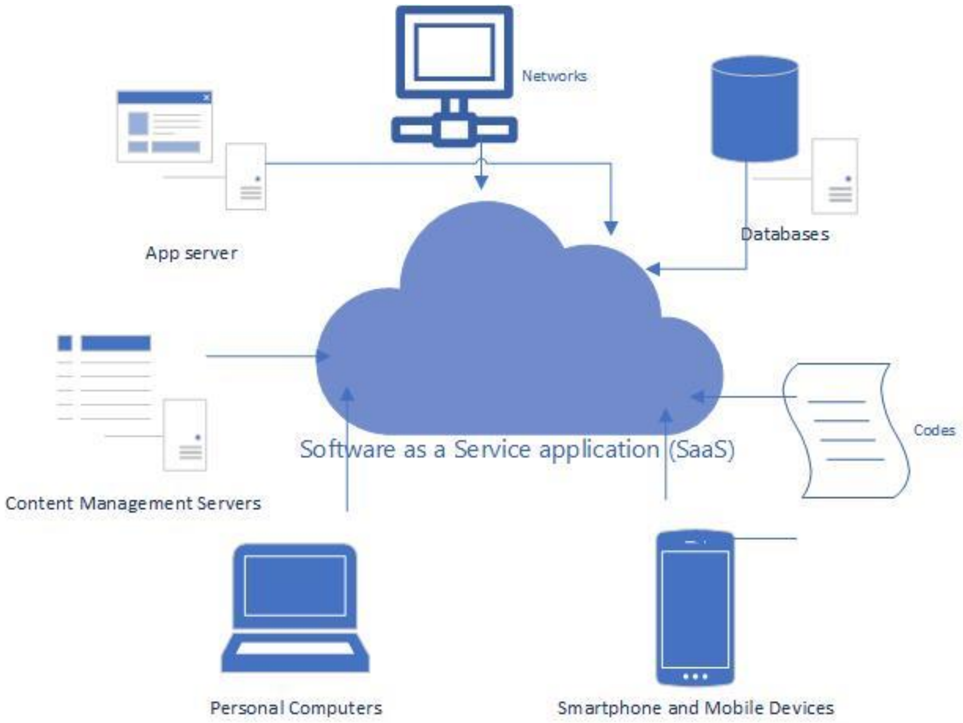

Networks
App server
Databases
Content Management Servers
Software as a Service application (SaaS)
Codes
Personal Computers
Smartphone and Mobile Devices

Figure 2: SaaS model (NIST,2011)

According to (R. Maheshwari,et al. 2020, Ojala, 2014, CSA, 2017, NIST, 2011, Loukis, Janssen et al. 2019, NIST Guide , H. Song, P. H. Nguyen et al. 2019, Singh, S., Jeong et al. 2016), and (G. Laatikainen, A. Ojala 2014), the SaaS architecture is sometimes divided into a number of categories referred to as maturity levels. These levels are the ad-hoc level (J. Jing, J. Zhang 2010), the configurability level (D. Li, W. Zhang et al.

2011), and the multi-tenancy level (Zhang et al. 2011), a critical level where more than one user shares the same application and hardware. It is at the multi-tenancy level where the application differentiates between application tenants as well as their usage data, and configurations (Komu, Sethi et al. 2012), (X. Zheng, J. Jiang et al. 2017). Tan *et al.* (Tan, Ai 2011) described a multi-tenant environment as having multiple users of a SaaS application who may be from different locations. Organisations may use the same application but may also be prevented from or not capable of seeing or having access to each other's configurations and usage data. They may still be allowed to share the same application and scalability, which is a significant issue that SaaS applications face. Numerous organisations (tenants) typically share each SaaS application, with each tenant having hundreds or thousands of users (Yimam, Fernandez 2016), (CSA 2017), (S. Aleem, et al. 2019), (Sultan et al. 2019).

SaaS applications represent the largest group of applications in the cloud market and can be divided into two variations, horizontal and vertical (Hinkelmann 2018). Horizontal applications are email or collaboration applications. They can encompass different industries and markets. Meanwhile, vertical SaaS applications are targeted to industries such as oil and gas, healthcare, and financial and banking industries. (R. Maheshwari, et al. 2020) described horizontal-based SaaS applications as those that are mainly focused on wide adoption, whereas vertical SaaS are those that are mainly focused on industries.

SaaS applications offer numerous benefits and efficiencies in some use cases, such as collaboration technologies (J. Tarazi, V. L. Akre 2013), (E. Huanachin-Yancce, R. C. Vega et al. 2019), customer relationship management systems (A. Manchar, A. Chouhan 2017), (M. Rezaei-Malek, N. Rezaei-Malek et al. 2013), retail sales (A. A. Achargui, A. Zaouia 2016), billing, enterprise resource planning, human resources, social networks (A. Nugraha, et al. 2012), financials, (A. Shi, Y. Xia et al. 2010), content management (*IEEE Standard,* 2018), email (Radicati, Levenstein 2013), and office productivity (P. Xu, T. Jiao et al. 2016). Because of these benefits, there has been a significant rise in interest in SaaS applications and other cloud technologies, with (Gartner Inc 2019) SaaS revenue reaching about $85.1 billion in 2019 as SaaS applications continue to provide incentives for adoption such as low cost, pay as you go, pricing models, quick setup, scalability, and easy upgrades to businesses and organisations (Harikrishna, and Amuthan, 2016).

2.2 SaaS Use Cases

2.2.1 Collaboration

As one of the SaaS model use case, collaboration has become a means for improving organisations' productivity and output. Collaboration technologies form an essential part of organisations' infrastructure and investments, especially in essential areas such as supply chain management, retail, banking operations, educational and knowledge management, teamwork, and process improvement (J. Tarazi, V. L. Akre 2013). Some of these collaboration applications relying on the SaaS model include Microsoft Sharepoint (Huanachin et al. 2019), Monday.com (Monday.com 2020), Blink.com (Blink 2020). Because user data are communicated as plain text in SaaS applications, in this context, data protection becomes very difficult by relying on existing security, privacy, and data protection methods (Volmer, 2018).

2.2.2 Customer Relationship Management (CRM)

The dawn of the cloud brought a significant shift in how organizations manage relationships with their customers. In the past, organizations used a model of the onsite or on-premise client-server applications to manage relationships emanating from a sale. However, today, the SaaS model has significantly impacted that model, and now customer relationships are managed using customer relationship applications or CRM. CRM applications allow organizations to collect, store, and manage clients' data using the SaaS model to track each customer's collaboration, including future customers and relationships (Chouhan, 2017). One of the SaaS applications aimed at CRM is Salesforce. As a CRM application, Salesforce helps organizations organize data into objects and records (M. Rezaei-Malek, et al. 2013).

2.2.3 Retail and Sales

As one of the use cases of the SaaS model, many companies rely on some forms of enterprise SaaS applications to drive their sales in their retail business, such as in logistics, supermarkets and food chains, oil and gas, and pharmaceuticals. As retail organizations are complex due to the complexities of the relationships and partnerships they rely on, SaaS applications have continued to help them scale by relying on the SaaS model's scalability model of the cloud-computing paradigm. Following this trend, enterprise software vendors move from single-tenant on-premises applications to multi-tenant SaaS applications to sales and retail sectors (Nguyen et al. 2019).

2.2.4 Enterprise Resource Planning

Another use case of the SaaS model is enterprise resource planning. As more organizations migrate from on-premise, client-server architectures to SaaS-based solutions, ERP providers began to provide best business processes using the SaaS models. Due to the consequence of adopting the SaaS delivery model, previous ERP applications were only affordable to enormous organizations. Now, the SaaS model has become affordable due to the cloud's pay-as-you-use model. ERP software or systems are modular applications that support different business functions utilizing fully integrated business processes by depending on a shared database; the visibility of data and collaboration increases among business units (Achargui, Zaouia 2015). For example, SAP Business ByDesign, Microsoft Silverlight, and Adobe Reader (J. Lewandowski, et al. 2013, Vinh Thong Ta, 2018).

Despite these benefits (Trapero, Modic et al. 2017), questions have continued to be raised around the security and privacy of personal data when using SaaS applications. These applications continue to suffer from several significant drawbacks and challenges relating to privacy and data protection, governance control, trust, identity and access management, incident response (Tiwari, Joshi 2014a), (NIST,2011) and data security (Y. Wang, et al. 2018).

To address these drawbacks and others relating to data handling best practices and data location (Vinh, 2018, Kovačić et al. 2018), governments and regional bodies such as the EU (Tamburri 2019), the Nigerian government (NITDA, 2019), and the United States have enacted data protection regulations (W. Stallings 2020a). These regulations have a significant impact on the operational activities of organisations concerned with personal data handling. However, compliance with these regulations continues to be a significant hurdle for users and service providers alike (M. Rueben et al. 2017).

2.2.5 Artificial Intelligence (AI)

AI is the science and engineering of creating intelligent devices, most notably sophisticated computer programmes (McCarthy 2007). Recently, SaaS applications have included AI to enhance the user experience in electronic commerce systems, for instance, (J. Tang 2020) developed an AI-based e-commerce system by relying on the SaaS model and neural networks to govern e-commerce market access, enhance the credibility of transactions, offer clear information to safeguard transaction security, and protect the interests of the transacting parties.

Similarly, (Ikram 2020) developed an AI-powered Service Broker for selecting simple and composite SaaS cloud solutions SaaS. Ikram stated that the solution includes a service ranking system, an evaluation system, and a composite decision-making system that assists SaaS service users to select the ideal service.

Additionally, (Hendradi, et al. 2020) claims that the evolution of education today recognises the term Education 4.0, which is an extension of the Industrial Revolution 4.0, in which the influence of Artificial Intelligence is critical. They then advanced an architectural design for an AI-based SaaS-based e-learning system that could serve as a model for Education 4.0.

2.2.6 Internet of Things (IoT)

SaaS applications are being utilised to power the Internet of Things (IoT) networks and devices (Antoniou, 2019). Recent forecasts indicate that over 30+ billion devices will be connected by 2023, and with the Internet of Things (IoT) at the centre of this growth, (Patel et al. 2019).

Today, as more data-capable devices are connected, new IoT applications driven by SaaS applications are emerging in practically every industry, including connected and autonomous vehicles (M. Hashem Eiza, Q. Ni 2017), logistics operations (Verdouw, et al. 2016) , both large and small.

The Internet of Things is a network of networks in which the end devices are not human-operated but may include devices, mechanical and digital machinery (Antoniou, 2019). Additionally, Antoniou argued that many firms now rely on IoT-based technologies to expand their capacity for providing superior customer service and streamlining management processes.

By utilising IoT to monitor an organization's operations and utilising software such as SaaS applications to track and collect data throughout the data life cycle, organisations can collect data on products and employees, raising ethical, legal, and human rights concerns, particularly regarding privacy and personal data protection. Antoniou then discussed the impact of incorporating IoT into a Smart Information System, such as an interactive SaaS platform, with a special emphasis on systems built to integrate with the 5G network.

Additionally, problems relating to quality of experience (QoE), legal and human rights concerns, such as data privacy, were analysed and pertinent recommendations made in the context of an IoT and SaaS application enabled to track and gather data from the entire data lifecycle executed in a national and global case study.(Antoniou, Andreou 2019)

(López-Viana, Díaz et al. 2020) developed a prototype for a fully distributed system with a continuous delivery (CD) process flow for a customised SaaS application that distributes updates at the IoT Edge solution. IoT Edge is a computing solution for Internet of Things (IoT) systems that require rapid processing and reaction times in system to render real-time decisions (Morabito, Cozzolino et al. 2018), such as those used in smart farming . They then successfully instantiated the architectural model and CD process flow in a case study involving precision agriculture.

To address the problems of linked data in IoT domains (D'silva, Thakare et al. 2016) combined three open source technologies: Ejabberd, Apache Spark, and Neo4j database for usage by a SaaS application on a secure Microsoft Azure public cloud. To allow end-users to simply run their own IoT systems, (Nagano, Arai et al. 2021) introduced a new SaaS platform, Motch, to facilitate the operation of IoT systems created by end-users. The platform mainly addresses concerns at the stages of collection and storage of the data life cycle.

2.3 The Concept of Privacy

In the past, the idea of privacy played a critical role in the political, economic, social, and even religious scholarship of early scholars. The concept of privacy has been discussed in the works of philosophers such as Aristotle and Locke. Locke's argument on private and public property concepts provided the basis for a clear differentiation between private and public property. Locke explained why he denoted the description of private property as a characteristic of privacy (DeCew 2015).

As human society advanced, especially in human rights, this led to the adoption and recognition of many rights – particularly the individual's 'right to be left alone' (Solove 2005). This is further highlighted in the works of two leading scholars on the concept of privacy, (Warren, Samuel D., Brandeis 1890), who argued that a person has the right to their privacy, including the body's privacy and mind. Further, they argued that this right is enforceable, and it is known today as the individual's right to privacy. With today's technological advancements, such as the cloud and artificial intelligence, old arguments on privacy, such as the individual's right to not be observed or even disturbed (Curzon, Almehmadi et al. 2019), are no longer tenable.

From a legal perspective, countries, regions, and bodies have advanced different definitions of privacy. For example, the EU has given the concept and right of privacy for EU citizens the law's backing by setting up the EU Human Rights Commission (Drake 2017), (Goddard 2017).

These rights were also included in additional EU initiatives such as the Convention for the Protection of Individuals in 1980; data protection directives (Markopoulou, Papakonstantinou et al. 2019); and, recently, the GDPR (Custers, Sears et al. 2019, Albrecht 2016) repealing early directives and conventions (Custers, Sears et al. 2019). With the evolution of these conventions and directives, legal rights relating to the individual's right to privacy were granted and guaranteed in law, while at the same time, obligations were imposed on organisations that collected and processed the personal data of EU citizens.

Other regions and countries followed suit, enacting data protection regulations in places such as Nigeria (Asuquo 2019) and the United States (Maria, 2020), requiring organisations to implement privacy principles for their products at the early stages of their development and specification.

As explained earlier, today's evolution has enabled many ways of observing the individual and violating their right to privacy well beyond the physical sense. For instance, several technologies today collect information relating to an individual shared or accessed – sometimes in violation of the individual's privacy.

Brandeis *et al.* (Westin 1968), (Warren, Samuel, Brandeis 2019) argued that privacy is an individual's and, sometimes, an organisation's ability to define when clearly, the means through which and the degree to which their data are shared with others. This definition is also in line with Westin's, a leading voice on privacy (Westin 1968). Altman (Westin 1968) made another argument about privacy where he argues that privacy can be understood as a situation where there is a degree of selective control over how information about an individual is accessed. He further argued that privacy is not absolute by itself, and that it can be further classified or categorised at some desired levels, such as solitude, wherein an individual is free from being observed; intimacy, an individual’s experience with another individual; anonymity, an individual’s experience while in a public space; and reserve, a barrier that prevents or counters intrusions into privacy. Therefore, to protect an individual's privacy rights, the individual should be able to obtain solitude, intimacy, and anonymity without having to resort to reserve (Breaux, Pearson 2016), (Altman 1975).

Margulis and Stephen (Margulis 2003) explained that privacy is the degree of control an individual exerts over a transaction involving their privacy with the intention of gaining increased independence or autonomy while reducing their vulnerability to privacy violations.

Many experts have tried to explain the concept of privacy within the context of their professions, such as medical practice. However, currently, there is no single, all-encompassing definition of privacy, specifically in academic research (Xu, Dinev et al. 2011), (Phelps, Nowak et al. 2000), further lending support to the argument that privacy itself has many sides to it, and therefore, it is multi-faceted (Burgoon, Parrott et al. 1989, Breaux, Pearson 2016). The term itself is wide-ranging and can be further divided into decisional and constitutional privacy. These relate to how a person exercises their freedom to make choices on personal issues, such as a spouse's choice. Personal data privacy refers to an individual’s control over how their personal data are accessed (Van der Sloot 2017).

In this research work, privacy, namely, personal data privacy, is considered within the context of new technologies such as the cloud and, in particular, SaaS applications. Therefore, as argued earlier, the existing literature on the concept of privacy, especially the early literature, cannot grapple with the new challenges of privacy in the age of the internet, distributed computing, cloud computing, and SaaS applications (Austin 2003). The internet and new technologies have increased data privacy's scope and reach to incorporate the electronic and digital environment, thus further amplifying data privacy concerns and motivating individuals to solely control access to their personal data on electronic and digital platforms (Smith, Dinev et al. 2011).

2.3.1 Definition of Personal Data

According to Butin (Butin, Métayer 2015), personal data are any information that can be used for identifying an individual, such as identity information, health information, financial information, political ideas, and religious beliefs (Saatci, 2019). Further examples of personal data include a person’s name, date of birth, and other indirectly identifiable records used daily, such as telephone numbers, social security numbers, images, preferences, family information, email addresses, fingerprints, group memberships, and IP addresses (Saatci, 2019). Understanding how personal data are described or defined is key to understanding how regulations such as the NDPR and GDPR are executed. The NDPR defines ‘personal data’ as:

> Any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; it can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, International Mobile Equipment Identification number (“IMEI”), IMSI number, SIM, personally identifiable information and others (Nigerian Information Technology Development Agency 2019).

Privacy is defined in Article 4 (1) of the GDPR as sensitive information that can be directly associated with a natural, identifiable person. Similarly, the NDPR defines it as information on one's sexual life, health, political thought and groups, beliefs, religion, convictions of a criminal nature, biometric data, fashion and clothing choices, philosophical beliefs, race, union or group memberships, ethnicity, sect, and so on. If any unauthorised person accesses this personal information, the owner may suffer discrimination and victimisation. Therefore, it is important to guarantee an individual's personal data privacy.

2.3.2 Data Security and Privacy

As security is an ever-evolving concern, especially in the cloud, and it has continued to be a significant inhibitor to SaaS applications' adoption as concerns for data privacy and protection linger. Due to the SaaS application's architecture, service providers collect personal and usage data and warehouse them on their hosting platform. The security of the collected data remains a challenge to organizations and users. Hence, an organization has to trust the service provider to store and protect its private data safely. However, many things can go wrong with data kept in infrastructure and a location that cannot be verified. For example, a SaaS service provider's business might cease to exist or it might outsource data storage to a third-party infrastructure service provider who may not have any contractual obligation to the data owner.

Likewise, with regards to privacy, Culnan and Mary (Culnan, 2003) stated that data privacy is the ability of the data owner to have the means or wherewithal to decide how their personal data are used. This contrasts with the early perceptions of privacy by Westin (Westin 1968), (Altman 1975). Today, a user or data owner on an electronic or social platform may argue that violations to his privacy can be established if he loses his ability to control certain operations on his data. To that effect, Obrien *et* *al.* (O'Brien, 2012) argued that in an electronic or digital environment, a user's data privacy can be violated once they lose control of the data in the environment.

While some scholars have identified control over their data as the most important concern users have, a substantial number of people continue to share their personal information on media platforms such as Facebook and Twitter (Rosenblum 2007). Depending on the type of data and user, users of technologies such as the cloud and SaaS applications may be particularly worried about data privacy. This is particularly the case with enterprise users of SaaS applications (Breaux, Pearson 2016).

Article 29 (Ni Loideain 2016) of the GDPR mentions the loss of control over data privacy and other factors, such as vendor lock-in and the attendant risks of unauthorised access to personal data, as some of the challenges users face. These challenges affect their decision to adopt services such as SaaS applications. To help integrate privacy into technologies and systems, the privacy by design principles were proposed by (Cavoukian, Chibba 2018).

2.3.3 Privacy by Design Principles

Experts and industry bodies have advanced a number of privacy by design principles to facilitate the implementation of privacy by design. Cavoukian, Schaar, and industry bodies such as the ISO/IEC 29100, for example, have advanced these principles. Kamocki, (2020), Cavoukian, (2018) defined PbD as the philosophy of including privacy principles early in the stages of design and specification of a technology or solution. Cavoukian advanced seven principles that later became the foundation of privacy by design philosophy. Recently, she provided a simplified framework for the continued implementation of the seven principles. Cavoukian stated that major equipment producers such as IBM have generally accepted privacy by design. Furthermore, she argued that privacy and, by extension, data protection can be achieved when the seven principles are customised to reflect an organisation's requirements and the technology or systems under consideration (A. Cavoukian 2020).

Similarly, Everson (2016) advanced six objectives relating to preserving privacy when designing systems. He argued that system designers, manufacturers (A. Cavoukian 2020), and developers should be encouraged to reflect on these objectives when designing or building a system or technology. At the industry standards level, the International standard organisation (ISO) introduced the ISOO/IEC 29100 with about 11 principles. In the table below, these principles are compared to the guidelines and directives of the GDPR and NDPR.

Table 1: Comparison of the NDPR and the GDPR

S/N	NDPR (2019) Guidelines	Ann Cavoukian (Privacy by Design (A. Cavoukian 2020, Asuquo 2019, Everson 2016))	GDPR (2018) Guidelines	OECD Guidelines	EU/95 Directives
1	Implementing key principles of the NDPR, such as obtaining **lawfulness consent** before data collection and establishing **transparency**	Being proactive and not remedial	Implementing key principles of the GDPR, including establishing a lawful basis, obtaining consent, ensuring fairness, and establishing transparency	Limiting data collection	Ensuring **fair** and **lawful** data processing
2	Establishing **due diligence** and clear evidence of **purpose** for data collection	Implementing privacy settings in default mode	Limiting personal data collection to collection purpose	Guaranteeing quality of data	Having an explicit, specific purpose for data collection
3	Minimising personal data collection	Embedding privacy into the design	Minimising personal data collection	Having a specific, clear **purpose** for data collection	Obtaining measured and adequate information relating to the purpose of data collection
4	Limiting **retention** and **storage**	Ensuring full **functionality**	Limiting personal data storage	Limiting data usage	Not **retaining** and **storing** data longer than required
5	Ensuring the **confidentiality** and **integrity** of personal data are maintained	Implementing security in the entire **end-to-end life cycle**	Establishing data **integrity** and ensuring its **confidentiality**	Guaranteeing **safeguards** concerning **security**	

6	Making sure that personal data are **accurate** and **error-free**	Ensuring **visibility** and openness	Ensuring the **accuracy** of data	Establishing **openness** and **transparency**
7	Designing and implementing a **compliance mechanism**	Ensuring focus on the user and respecting **user privacy** preferences	Holding data processors accountable to their legal obligations	Ensuring **inclusion** and participation of **individual**
8	Protecting data by implementing mechanisms by default		Ensuring data protection by design and by default	Accountability

According to the comparison in Table 1, consensus on privacy and data protection principles has not yet been established. However, there exist many similarities between the NDPR, the GDPR, and Couvakian's updated privacy by design principles. Therefore, because the focus of this thesis is the NDPR, the seven principles of the NDPR will be used for the subsequent design of SaaS-PPL based on the PPL structure.

Part 4 of the NDPR and Article 25 of the GDPR note that data controllers and processors have to integrate data protection mechanisms (Asuquo 2019) and principles into their products. Data protection requirements are listed and defined in Parts 1 and 2 of the NDPR and Article 25 of the GDPR.

Therefore, to further ensure clear alignment of the GDPR data protection principles and the NDPR principles concerning PbD, the researcher compares the two (see Section 2.5). The NDPR principles will be used to specify the properties of the SaaS-PPL and specify compliance requirements based on privacy by design principles in the context of this research, namely, SaaS applications.

Table 2: NDPR requirements

S/N	**Notation**	**NDPR Data Protection Principles**
1	NDPR1	Ensuring legitimacy, obtaining lawful consent, and ensuring transparency
2	NDPR2	Establishing **due diligence** and clear evidence of **purpose** for data collection
3	NDPR3	Minimising personal data collection
4	NDPR4	Limiting **retention** and **storage**

5	NDPR5	Ensuring the **confidentiality** and **integrity** of personal data are maintained
6	NDPR6	Ensuring that personal data are **accurate** and **error-free**
7	NDPR7	Designing and implementing a **compliance mechanism**
8	NDPR8	Protecting data by implementing privacy and data protection mechanism **by default**

2.3.4 Methods to Implement Privacy by Design

There is currently a gap between these principles and their actual implementation in systems and technologies. This gap has continued to challenge experts, manufacturers, and developers when integrating privacy by design into their systems (Kung, Kargl et al. 2017). (Johannesson, Perjons 2014)

Recently, Cavoukian attempted to simplify implementing the seven foundational principles, citing the real-life experiences of organisations and experts when implementing privacy by design, including the need to take into account the unique requirements of diverse organisations (A. Cavoukian 2020). Several attempts, methods, case studies have attempted to implement these principles on their processes, technologies and platforms.

These approaches include managing privacy in management processes and engineering and technology. Sangyhu *et al.* (2018) proposed a new Privacy Impact Assessment manual for meeting the requirements of ISO/IEC 29134:2017, and Métayer (2016) proposed a rigorous and systematic privacy risk assessment methodology. The methodology was demonstrated as a quantified self-use-case (Martín, Del Alamo et al. 2014). Similarly, Berendt, et al. (2005) and P Schaar (Schaar 2010) demonstrated how privacy by design can help improve data protection and how privacy protection can be incorporated into the overall design (Deng, Zheng et al. 2018), (ElShekeil, Laoyookhong 2017).

Alshammari *et al.* (Alshammari, 2018) proposed privacy by design method that relies on architectural strategies for supporting the adoption of privacy-enhancing technologies, particularly at the nascent stages of design, to achieve privacy assurance. Notario, et al. (2015) conducted a comprehensive review of the best ways, means, and practices for successfully implementing privacy by design in systems. He argued supporting implementing privacy early in the development life cycle of a technology, system, or solution and introduced a methodology for privacy engineering (Notario, Crespo et al. 2015).

Similarly, (Gjermundrød, et al. 2016) advanced a privacy by design framework to achieve compliance with the GDPR and perform data traceability and implement controls based on the traces. Similarly, (Ferrara, 2018) proposed a GDPR and static analysis, arguing that algorithms can be combined to generate reports that help achieve privacy through design compliance with the GDPR.

2.3.5 Challenges to Privacy by Design

The concept of privacy by design remains relevant, although different views on implementing the concept have been advanced, especially in new contexts such as SaaS.

No single approach or framework is covering all the stages of privacy and data protection. This challenge and general lack of consensus may exist because privacy itself means different things to different stakeholders. Spiekermann et al. (2012) contend that privacy has become very tough to preserve or protect because it is a vague idea. They argued that stakeholders should find a way to achieve consensus, particularly on what should be protected and considered privacy protection.

Furthermore, Korunovska et al. (2018) stated that experts have some misconception or confusion about privacy, leading to them mixing up privacy and security. They argued for the need to distinguish the two to simplify addressing the privacy challenge clearly. They justified the need for a methodology to implement privacy in systems systematically and for a knowledge base on the risks and benefits companies derive from privacy practices (Bednar,et al. 2019).

Because of the above challenges and the lack of a strategy or method for implementing privacy in the cloud and SaaS applications scenario, Spiekermann et al. concluded that no established framework exists for meeting the legal and organisational requirements of privacy.

2.4 SaaS Applications and Data Privacy

SaaS applications consist of several layers that are responsible for transmitting and processing information over a network (Han, Kim 2017). These layers are also responsible for keeping data of applications and users private and secure (Tiwari, Joshi 2014a). SaaS applications are primarily in the service provider's possession, but they can be shared with users, which presents several privacy risks (Breaux, Pearson 2016). In Figure 3 below, an example of SaaS application service architecture is presented for an online retail platform that offers payment solutions and point of sale services to users.

In this scenario, the SaaS service provider procures services from another service provider, such as a broker. The broker pools several services from different SaaS service providers to create a service package, including advertisement and payment. In the course of providing these services, the SaaS retail provider may collect personal data and transactional data (Yimam, Fernandez 2016), including data from other partners in the service package (e.g. the advertisement provider) to track users’ behaviours.

The SaaS retail service provider may work with several advertising and storage services that process payments and offer services. Figure 3 illustrates how personal data are collected from the customer or user and shared with different services to deliver an end-user experience. Additionally, the data may be stored by other service providers, such as storage service providers who may not have any contractual obligations with the data subject.

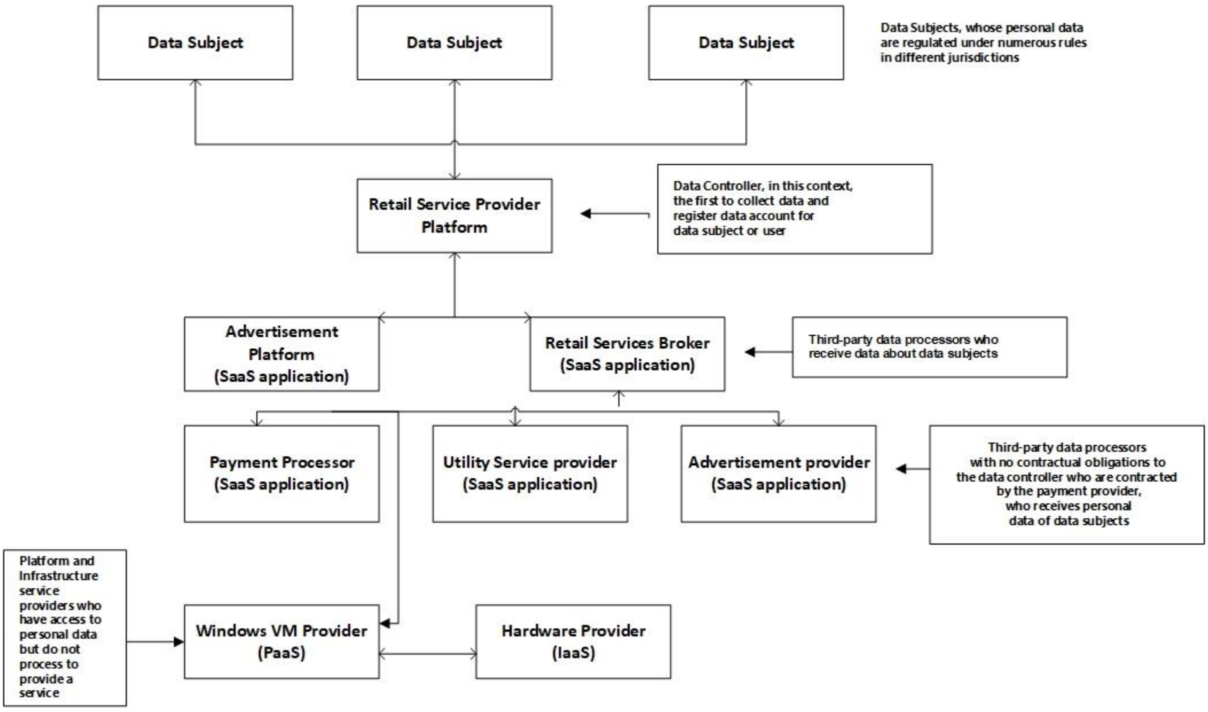

Data Subject
Data Subject
Data Subject
Data Subjects, whose personal data are regulated under numerous rules in different jurisdictions
Retail Service Provider Platform
Data Controller, in this context, the first to collect data and register data account for data subject or user
Advertisement Platform (SaaS application)
Retail Services Broker (SaaS application)
Third-party data processors who receive data about data subjects
Payment Processor (SaaS application)
Utility Service provider (SaaS application)
Advertisement provider (SaaS application)
Third-party data processors with no contractual obligations to the data controller who are contracted by the payment provider, who receives personal data of data subjects
Platform and Infrastructure service providers who have access to personal data but do not process to provide a service
Windows VM Provider (PaaS)
Hardware Provider (IaaS)

Figure 3: SaaS architecture including relationship overlap; Travies et al. *(Breaux, Pearson 2016)*

As explained above, SaaS application service providers take advantage of third-party hosting services (Trapero, Modic et al. 2017). However, they must make transparent which countries they are hosting their user's data, and the privacy laws governing their data handling practices. For example, an organization operating in the EU is obligated by the GDPR to ensure that its operational and personal employee data are located in Europe (Altorbaq, Blix et al. 2017a). Therefore, the organization would want to know how the GDPR is applied in the storage of private data.

Moreover, an organization based in Germany may want to subscribe to a SaaS application service hosted in the US.

Nevertheless, the organization would be objected by the law to the transfer or store its data to other locations outside the EU due to privacy concerns (Sultan, 2016). Therefore, the knowledge of where a SaaS applications service provider will keep the application and storage data becomes a prerequisite to how data is transferred across borders (S. S. Ghuge, N. Kumar et al. 2020). Regulations governing the privacy of data have become an essential factor in decision making (N. Kshetri, and S. Murugesan 2013).

As SaaS applications service providers continue to rely on multi-location and dispersed storage infrastructures, processing and storing personal and application data is performed in remote and diverse locations, which adds to the complexity of compliance as personal data traverses different jurisdictions and becomes more vulnerable to privacy violations (Kulkarni, et al. 2013, Ashalatha, 2016). Consequently, potential privacy issues and challenges have become vital for organizations and users to protect their private information, particularly personal data (Kittmann, et al. 2018). Thus, the protection of particularly personal data has become a significant problem that requires attention. Today's business environment requires organizations to personalize user experiences to cement the relationship with the user because user experiences are used to customize experiences based on a user’s preferences and choices (Fujita, Harrigan et al. 2020).

Within the background of this research, clear definitions have been established for personal data. They are referred to as any information that can be used to identify a living or natural person as a data subject in the NDPR (NDPR, 2019). Additionally, any organisation or entity that determines the purpose of data collection and processing of personal data is defined as a data controller, and any organisation that processes data in an arrangement with a data controller is defined as a data processor (Agbali, Dahiru et al. 2020).

The SaaS retail platform depicted in Figure 3 collects personal data that is then shared with other partners for processing, who may, in turn, go on to process personal data for other services with their partners without any input or consent from the data subject.

Breaux (2016) argued that sharing data across services and providers may be a good business strategy to scale up processing and delivery capabilities and even save costs. However, it presents a significant privacy challenge to data subjects, whose rights as service providers relating to privacy may easily be overlooked because of the difficulty of determining who should take direct responsibility for data privacy under such a diverse scenario.

In Figure 3 the service provider has more control over the data processing, so it must implement security controls. However, data processing providers who provide the only infrastructure still have access to personal data, so they must implement data protection controls.

In SaaS applications, a service provider usually has more obligations, but in a situation where the SaaS provider relies on other service providers to provide a service, the other service providers may come into contact with private data (Park, Hwang et al. 2015). This necessitates the implementation of controls such as data protection. Similarly, in a situation where at least two models of the cloud are used, such as a virtual machine where a SaaS application with a multi-tenant architecture is hosted, the virtual machine provider may not know who the SaaS applications' users are but may still be obligated to implement privacy controls (Brodin 2019b) .

Primarily because SaaS applications can be scaled as services are streamlined, data users face a loss of transparency and control (Yu et al. 2018). To reduce privacy risks, while signing contracts, the provider should promise to implement privacy safeguards and establish privacy guidelines from the early stages (Vinh, 2018).

In the example above, the data controller relies on service level agreements (SLAs) to provide assurances that its direct and indirect processing partners are adhering to the retail platform privacy expectations of customers or users. Protection of user privacy is maintained mainly through contracts with service providers. Most privacy policies are written for end-users, but specific policies can be drafted for specific users. For individuals and small business, there is little, if any, bargaining power in these small contracts. Thus, data subjects depend entirely on data controllers to guarantee their data integrity in other cloud services.

Within the SaaS context, privacy questions that may arise with SaaS-based services include where data are located and how that would affect data subjects' rights. Another question is, to what extent are third-party service providers given access to the data?

For instance, to what degree will the SaaS provider and its stakeholders be able to use data? What protective measures are SaaS services using to ensure the availability, integrity, and confidentiality of data? For how long are data retained, and are they backed up? What method does the SaaS provider use to handle consent, including giving data subjects the ability to access the data needed to comply with data regulations or make certain users eligible for the removal of contested data? Because data in SaaS applications relate to payments and other personal data, they have mass value and are increasingly a target for harmful activities. Similarly, (Subashini, Kavitha 2011) further surveyed specific security issues relating to the SaaS model and described poor data security as a significant impediment to cloud and SaaS adoption.

2.5 Data Protection

Data protection is defined as legal restrictions placed on third-party access and use of personal information. The idea of privacy legislation was first introduced in Europe in the context of data protection. Laws protecting data go back to the 1970s when personal data processing became prevalent among businesses (Dinev 2014).

Sion *et al.* (2019) termed comprehensive data protection as a collaborative activity that incorporates subject matter experts, computer engineers, compliance engineers, and system programmers in the design and development process. Various privacy laws call for controllers to be meticulous when handling personal data. However, data protection has several barriers, including the acquisition of consent, use of personal data, processing, archiving, right to erase, and organisation data transfer to third parties.

In cloud platforms, data are always co-located with other users. Storing sensitive information in the cloud environment, such as SaaS applications, necessitates understanding how it is accessed and kept secure. Rajeswari *et al.* (2017) described critical challenges of data privacy and security in the cloud computing era. They contended that private information might be accessed in the cloud because of a lack of privacy and data protection mechanisms. They surveyed and analysed each category of existing security and privacy solutions and compared its strengths and weaknesses.

Additionally, Subashini *et al.* (2011) further surveyed specific privacy issues. They argued that because of data privacy and protection issues, the growth of SaaS is being impeded. They reviewed security threats that SaaS applications face, including threats originating from service models such as SaaS.

Mazhar *et al.* (2017) also surveyed the many privacy challenges SaaS faces and highlighted data backup as a crucial challenge that must be dealt with carefully. To ensure data availability and recovery, and data protection, they recommended backing up data regularly on the SaaS application service provider’s platform.

2.5.1 Data Protection Laws, Regulations and their Implementation

For SaaS applications, recent security and privacy compliance regulations include the NDPR, GDPR and CCPA. Others are the privacy act of 1974, Federal Information Security Management Act (FISMA) of 2002, E-Government Act of 2002, and National Archives and Records Administration (NARA) statutes and regulations. Other industry standards and frameworks include ISO/IEC 27000, Control Objectives for Information and Related Technology, Payment Card Industry Data Security Standard, and Cloud Control Matrix. Here, a summary of some relevant regulations such as the NDPR, GDPR and CCPA directly impact the SaaS model.

Similarly, DLA Piper (DLA Piper, 2020) , an expert on data protection laws, created a web-based app to provide an overview of the level of data protection in different countries. The company indicated that it is currently reviewing regulations in this area of data protection and implementing it across the World. Additionally, it focuses on regions with explicit or extreme data protection regulations, as stated in the DLA piper web application.

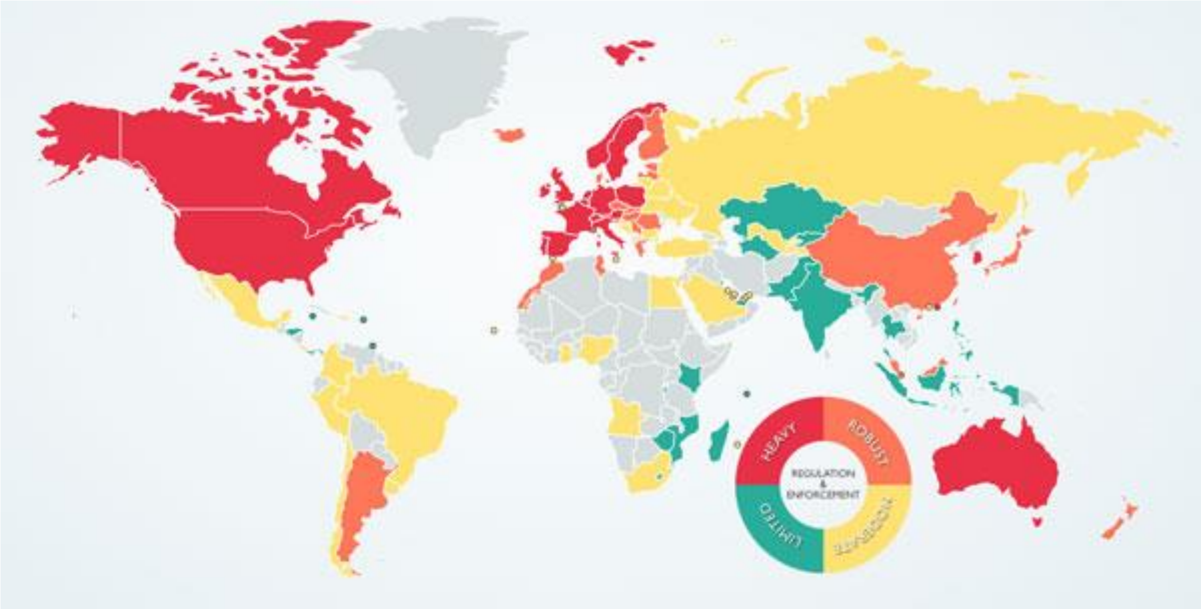


Figure 4: DLA Data protection laws of the World 2019(Chris Dale)

Yimam and Dereje (2016) described data protection regulations as rules for implementing specific legislation relating to data security that is formulated and maintained by the authorities. These data regulations are unique to their purposes and countries of origin, but according to (Giulio, et al. 2017), they are similar and designed to achieve local needs in many cases. The NDPR is like the GDPR in many areas; for example, both aim to guarantee reliable protection of individuals' personal data from organisations that collect, use, and share such data. Other similarity areas include their scopes, definitions of key terms, legal bases, and recognition of rights and their enforcement. At the same time, they are different in other areas, especially in enforcement and implementation. For example, member countries of the EU implement the GDPR through an independent body such as the Information Commissioner's Office (ICO, 2019c). Meanwhile, the Federal Government Ministry of Communication implements the NDPR via the Nigerian Information Technology Development (NDPR, 2019). In the current research work, we consider the NDPR.

The NDPR (2019) states the rights of people who are living and whose data are processed. They also specify the responsibilities of data controllers who process and handle personal data (Altorbaq, et al. 2017b). Because of the impact of the NDPR, organisations are now concerned about compliance when adopting software technologies such as SaaS applications.

2.5.2 The NDPR (2019)

The NDPR and GDPR both serve to strengthen individuals' protection of their data, and both apply to organisations that collect, use, or distribute data within their territories.

The NDPR came into effect in April 2019 (NITDA, 2019). The regulation aims to safeguard natural persons' data privacy rights and transactions, including the transfer of personal data, and to keep personal data from being compromised.

NDPR aim to ensure that businesses in Nigeria stay competitive in international trade. Thus, the regulation puts in place both legal and regulatory safeguards regarding personal data protection. The coverage of the NDPR extends to all transactions involving the personal data of natural persons in Nigeria. There is a penalty for violations: 2% of annual revenue for those data controllers who are accountable for more than 10,000 data subjects and those who control fewer than 10,000 data subjects.

2.5.2.1 NDPR Analysis Outcome

Organisations such as SaaS application service providers in Nigeria generally collect users' data via email, application usage cases, website engagements, and, sometimes, via telephone (Agbali, Dahiru et al. 2020). The types of data they collect include name, date of birth, and bank or credit card information (Izuogu 2021). Additionally, they process orders using secure technologies while collecting customers' bank information.

Service providers process data in a number of ways: (1) storage, (2) using or processing personal data such as in processing payment processing, (3) promotional and third-party data sharing, and so on (Ibrahim, et al. 2018a). Although many kinds of organisations process their employees' data, this study is not concerned with them. One of the essential premises of the NDPR is that organisations collect only those necessary data, which raises whether the data that data controllers or processors collect is relevant to their purposes (Vincent 2020).

One of the most essential principles of the NDPR is that personal data must be discarded as soon as they are no longer needed (Asuqu, 2019). For example, the user's name, address, or telephone number are typically required only for payment processing, but requests for details such as the user's date of birth and nationality may be difficult to justify (Rantanen, et al. 2020).

Service providers may only retain personal data for a period where a clear lawful justification continues to exist (Pandit, et al. 2018). If the service provider has fulfilled a service request, it cannot keep promoting or marketing services to the user indefinitely. A service provider or organisation may only retain personal data where there is a legal obligation to do so based on the stipulated maximum retention period described in the NDPR principles (Izuogu, 2021).

2.5.2.2 NDPR Legitimate and Lawful Bases/Principles

Organisations must have the legal right to process personal data. Some legal bases for personal data processing are specified in the NDPR, but it is absolutely necessary for service providers to demonstrate specific legal grounds for each type of personal data they use. The NDPR lists eleven valid legal grounds for handling personal data (NDPR, 2019):

- Personal data may be processed only with the explicit consent of the data subject.

- The data subject will be required to give explicit consent to have their personal data processed.
- Personal data may be kept only for the duration during which they are required.
- Personal data should be secured against foreseeable hazards and breaches.
- Personal data processing may be required to execute service delivery on behalf of the data subject.
- Due diligence and prohibition of improper motives are required.
- Lawful personal data processing is a legal obligation, and compliance purposes before service delivery.
- Personal data processing should be for the benefit of the subject, such as when the subject is facing a matter of life and death.
- Personal data processing should be in the public interest, such as the exercise of official authority (e.g. policing and the administration of justice).
- Personal data processing may be required for the legitimate purposes of the data controller or processor, such as service delivery efforts in partnership with a third party.
- Privacy policies should be promoted and clarified.
- Third-party data processing.

Organisations must adhere to the above when collecting, processing, storing, retaining, and sharing personal data with third parties to fulfil a request or a performance of or honour a contract.

Based on these principles, the current research study proposes designing a policy language that can specify the properties of these legal requirements to ensure compliance to the NDPR to ensure security, privacy, and data protection compliance SaaS applications.

For example, a service provider may only collect personal data if evidence of free, specific, and informed consent has been obtained. Additionally, the user or customer must have the freedom to revoke consent at any time. This is a significant obligation and source of concern because the NDPR is a textual document, which makes ascertaining compliance difficult.

Next, service providers must demonstrate the legitimacy of their processing of personal data and ensure that user interests or fundamental rights do not supersede their processing purpose (NDPR, 2019). Ensuring that the NDPR's lawful and legitimate principles for each separate type of personal data processing are adhered to will require a mechanism to show proof of compliance. Service providers should also consider carefully implementing mechanisms that guarantee the security and privacy of personal data (Agbali, Dahiru et al. 2020).

2.5.3 The GDPR (2018)

The GDPR applies to European citizens and their data, regardless of where the data are held. It requires that data processing consent be explicitly obtained and that complete details of the procedure be provided. It designates EU citizens as 'data subjects' and describes 'data processing' as either an automated or a manual operation.

The GDPR's Article 4 describes personal data as any information associated with a natural person who is directly or indirectly identifiable. Article 4 (1) refers to the following list of identifiers associated with personal data: to include names; location data; genetic data; economic data; identification numbers; IP addresses; and cultural, physical, and social data. According to Volmer (Vollmer 2018), online IDs should be protected as devices because they are capable of leaving behind traces of user data, which can be used to target individuals.

A ‘data processor’ under the GDPR may be either a natural or legal person who processes personal data on behalf of ‘data controllers’, natural or legal persons who determine the purposes and methods of collecting personal data.

To ensure that data subjects have control over their data, they have been granted eight fundamental rights under the GDPR: the right to access in Article (15), the right to rectification in Articles (16 & 19), the right to erasure and to be forgotten in Articles (17 & 19), the right to portability in Article (20), the right to object to data processing in Article (21), the right to restrict processing and be informed in Article (18), the right to be notified or informed in Articles (13 & 14), and the right to automated processing and profiling in Article (22). Users have the right to object to any processing of their personal data for direct marketing purposes. These rights are enforceable, and in the event of a violation, data subjects can take their claims to the GDPR Data Protection Commission. According to Article 80 of the GDPR, individuals can also permit third parties to file complaints on their behalf. The commission may take several actions to resolve such complaints and may impose fines up to 10,000,000–20,000,000 euros or 2%–4% yearly revenue of the preceding financial year. Data subjects are permitted to pursue a legal claim against data controllers under the right to damages provision. In exceptional circumstances, they may even file criminal charges.

2.5.4 The CCPA (2020)

The California Consumer Privacy Act (CCPA) is a very effective state-level data protection regulation in the United States. It provides rights for protecting consumer privacy and controls how personal information is handled (PI) (W. Stallings 2020b). The CCPA was passed in June 2018, amended in August 2018, and became effective on the January 1, 2020. The CCPA went beyond existing privacy laws in the US to impact organizations that carry out their business and collect and process personal data information in the State of California, with noncompliance risking monetary penalties and other enforcement actions. It also empowered individuals to initiate a lawsuit for the breach of their data and privacy. The scope of the CCPA is aligned with three key areas, i.e., the definition of who is a consumer, specific industries covered by the CCPA, and the definition of what constitutes a PI.

2.5.4The ISO/IEC 27001

Information technology (IT) controls are reusable system requirements that IT managers rely on to prove compliance with international standards, such as ISO 27001 standard (ISO 2018). Moreover, as these controls are reusable, they lean toward best practices independently from what specific government laws may require. ISO/IEC 27001 is the international standard that describes best practices for information security management systems (Tjirare, and Shava 2017). ISO 27001 is buttressed by a code of practice (ISO 2018) and a wide-ranging security guide for organizations, including profitable enterprises of any size (Haufe, et al. 2018). According to (ISO, 2013), ISO has several security standards for different implementations and industries.

2.5.5 Payment Card Industry/Data Security Standard (PCI/DSS)

The United Kingdom Cards Association describes the PCI DSS as an information security standard set up to help organizations handle card payments securely to decrease card fraud (Elluri, et al. 2018a). The policy or standard guideline is designed for organizations handling data, e.g., debit/credit card numbers, sensitive authentication data (SAD) such as magnetic stripe data, and card schemes, card verification value (CVV), and primary account numbers (PAN) (The UK Cards Association 2018). The policy is only offered in textual format and incurs substantial manual effort to guarantee compliance. The standard has 12 high-level requirements, which fall into six categories (Yulianto, et al. 2016). The PCI DSS has a significant impact on SaaS applications, particularly in retail and payment services.

2.5.6 Cloud Control Matrix

According to (CSA 2017), the cloud control matrix (CCM) serves as a tool to help achieve the security, privacy, and data protection compliance requirements. It achieves that by listing controls and mapping them to numerous privacy, security, and data protection compliance standards. The CCM can similarly be used to record and identify data protection responsibilities (Elluri, et al. 2018b). The CCM and similar standards can be utilized in different sectors, e.g., retail, oil and gas, healthcare, finance, and government agencies. The CCM allows the organization of regulations' requirements, standards, and relevant industry best practices into controls and controls domain mapped to achieve security and privacy compliance (Giulio, et al. 2017, Jansen, 2011).

2.6 Compliance with Data Protection Regulations in SaaS

Compliance refers to conforming to established rules, regulations, guidelines, and specifications (Jansen, 2011). Based on the principles of shared responsibility applicable to the SaaS model, responsibility for the privacy, security, and protection of data rests with the user to a certain degree. Simultaneously, service providers are primarily responsible for securing their services, platforms, and infrastructures. Consequently, the general lack of control on the part of the user and the lack of transparency on the part of the service provider create an environment where compliance with data protection regulations is challenging for SaaS application service providers. SaaS application service providers have published and invested in compliance designs and implementations to improve transparency, e.g., the Microsoft compliance manager. These implementations are based on the service provider’s infrastructure and focus on their product offerings; therefore, they are provider or vendor-specific and do not follow common standard models and architectures.

In this regard, countries have enacted laws and regulations that will have a notable impact on how SaaS can be used as a cloud computing model. For example, the GDPR (Lee, et al. 2019) set in motion a new era of legislation governing the security and privacy of personal data. Several nations and regions administered by, for example, the NDPR, the GDPR, and the CCP (see Sections 2.5) and industry bodies such as the ISO (Shava 2017) have implemented similar data protection regulations to govern how personal data are handled within their jurisdictions.

According to Spasic *et al.* (2018a), different groups of users, including individuals and organisations, host and use SaaS applications in various countries, exposing their processing and usage of data to different rules and regulations. Therefore, data management and control are crucial to ensuring regulatory compliance.

In recent times, researchers have explored different approaches aimed at supporting organisations to achieve compliance with data protection regulations. These data protection approaches and solutions include policy frameworks and architectures designed to guard and enforce regulations such as the NDPR. For example, Jayasinghe (Jayasinghe, Lee et al. 2018) proposed a GDPR trust-based compliance framework for data controllers. Ta (Vinh, 2018) proposed personal data protection policies and architecture conformance checks. Similarly, Yu *et al.* (Winslett 2003) proposed a technical framework aimed at helping generate snapshots that are verifiable for compliance.

Additionally, Al-Zaben (2018) proposed an architecture that relies on blockchain technology to help manage personally identifiable information. Elluri *et al.* (2018a) advanced an integrated ontology that is semantically rich. This ontology represents in detail data protection regulations such as the GDPR. Indhumathil *et al.* (2017) put forward other forms of compliance regarding SaaS applications, they proposed third-party auditing of SaaS applications and argued that there is a relationship between the reluctance of organisations to use cloud-based services such as SaaS applications with privacy, security, and reliability concerns.

Similarly, Lins *et al.* (2018) argued that to increase the trustworthiness of cloud-based services, the practice of continuously auditing carefully selected criteria is helpful because it assures users of their data security. However, such solutions focus on trust issues, governance, and architectural and third-party manual auditing. They do not attempt to operationalise privacy by design requirements for compliance with data protection regulations in SaaS applications. Several approaches, such as manual auditing, third-party auditing, SLAs, and policy language approaches, are reviewed in this study.

2.6.1 Internal Auditors

Lierberman *et al.* (2002) argued that compliance can be achieved using internal auditors and that they are the best sources for identifying nonconformities within a system. They discussed the challenges internal auditors faced and suggested how they can help organisations achieve compliance and value. The drawback of this approach is that it is manual and time-consuming.

2.6.2 Third-Party Auditing

Indhumathil *et al.* (2017) made a case for third-party auditing in SaaS applications and cloud computing. They argued that organisations are still undecided about wholly accepting cloud services because of privacy, reliability, and security concerns. According to the authors, continuous auditing based on detailed certification criteria guarantees transparent, secure, and reliable cloud services, including SaaS applications. Moreover, Lins (2018) stated that certain certification conditions' constant auditing is essential to guarantee reliable and secure cloud services. It increases the dependability of cloud service certifications and ensures a high level of security and compliance.

2.6.3 SLAs

Another means of achieving compliance for cloud service providers is SLAs. They have been used for achieving availability, security, and privacy compliance in cloud and SaaS applications. Disi *et al.* (2009) explained that a critical component of services is the processes that establish and maintain compliance with SLAs. They designed a tool specifically for SLA compliance. Ismail *et al.* (2016a) agreed that SLAs could be relied on to guarantee the privacy and accessibility of outsourced information. Ibrahim (Ibrahim, Varrette et al. 2018b) developed a framework to guarantee SLA compliance in the web services that different cloud providers offer. The framework focuses on the quality of service (QoS) and appraisal of services (e.g. SaaS services) (Ismail, et al. 2016b).

2.6.4 Privacy Policy Language Approach

The privacy policy language approach to compliance with data protection regulations is majorly concerned with the specification and formalisation of privacy, data protection policies and requirements using policy languages. Further, Henze et al. (2016) described a policy language as the formalisation and expression of privacy and security policies into machine-readable languages. Additionally, Guilio *et al.* in (2017) described a security policy language as a language used in the specification of policies related to confidentiality and availability of data. On the other hand, a privacy policy language is used to create rules that can preserve and safeguard personal data privacy (S. Lins, et al. 2018)—for example, the extensible access control policy language XACML.

Khan (2013) developed a method to allow cloud-based clients to comply with health regulatory standards. The method enables clients to assess healthcare providers' compliance with HIPAA regulations. Similarly, Mandal (2018) discussed SaaS application security compliance's high-level goals in enterprises and proposed a novel approach for verification of compliance.

Various policy languages have been suggested for translation into human-readable and computer-readable formats. Some policies have been developed to express the service provider's privacy preferences, and others have been developed for users to define their privacy policies. Service providers can then use this set of user preferences to enforce users' data protection decisions. Generally, all policy languages are designed with particular syntax and semantics to simplify their implementation. However, no yardstick or metric exists that can be employed to analyse and assess policy languages. Ponnurangam *et al.* (2007) claimed that privacy policies could help with, for example, writing, reviewing, issuing, combining, modifying, withdrawing, and enforcing privacy policies.

A privacy policy language is usually designed to express the specific needs of both the involved parties, such as SaaS service providers and users, relating to security, access, authorisation, and data privacy. Further, most privacy policies are designed with specific purposes and aspects in mind. Heinz *et al.* (2016) argued that a policy language must fulfil a certain number of vital requirements to help specify policies in distributed environments with SaaS applications. These requirements, they claimed, include (i) policy checking, (ii) expressiveness, (iii) extendibility, and (iv) matching. To specify the privacy preferences of data subjects, a policy language is required.

Policy language initiatives started in 1997 with the platform for privacy preferences (P3P) (Olurin, et al. 2012) project for expressing privacy preferences in a machine-readable format at the Worldwide Web

Consortium. P3P was explicitly designed to express an individual’s privacy preferences, query the data P3P represented, and make decisions accordingly (Olurin, et al. 2012).

Similarly, CPExchange was developed in 2000 to enable business-to-business communication on privacy policies (Benghabrit, Grall et al. 2014). In 2003, IBM designed the Enterprise Privacy Authorization Language for achieving authorisation (Uddin, Islam et al. 2019) and the eXtensible Access Control Markup Language (XACML) for expressing privacy and security policies in a machine-readable format (OASIS 2017). Additional initiatives, including DPAL and XPref, followed in 2003 and 2004. With recent advances in technologies such as the cloud and, more recently, data protection regulations, there is a strong need for protecting sensitive data within specific jurisdictions and platforms.

According to Alshammari (Alshammari, et al. 2017), privacy policies are expected to be short and straightforward. For this reason, they are typically expressed in lightweight XML, which cannot convey complex mathematical operations. Similarly, Vinh *et al.* (2018) argued that policy languages could be used for specifying policies with relation to data confidentiality and availability, including the integrity of the properties of the data. At the same time, a privacy policy language can be used to create rules that preserve and safeguard personal data privacy (S. Lins, S. Schneider et al. 2018). For example, an access control policy language such as XACML is foundational but has remained relevant today. In this study, a few policy languages relevant to the research context are reviewed for modelling SaaS-based properties.

2.6.4.1 P3P Language

As indicated earlier, early policy languages such as P3P were designed as languages that provided a formal way of communicating privacy pledges to consumers. There are many P3P-enabled websites, as is evident from the fact that a P3P client is included in the Internet Explorer browser to allow privacy preferences communication. A service policy is a commitment to confining the usage of particular data to specific recipients and limiting how long the provider can retain the data. Before loading a web page's contents, the browser downloads the site’s privacy policy, which is also known as the site’s P3P policy and compares it against the consumer’s preferences. If the privacy policy preference complies with the user’s preferences, the browser will load the website. However, if the user’s preferences are not respected, the browser will not load the website (Adams et al. 2012).

2.6.4.2 XACML

XACML, as indicated, is an access-control-centred policy language. It has an inbuilt request/response language for effective two-way communication (Ardagna, et al. 2010). Additionally, XACML comprises mainly generic XML elements and generic points for precise rules relating to access, varying data types, and authorisation procedures. Because of its standardisation in the Organisation for the advancement of structured information Standard (OASIS), many access control schemes exist. For example, these extensions include profiles for usage control (OASIS 2017), privacy policies (M. M. Krupp, M. Rueben et al. 2017), PPL (Trabelsi, et al. 2011), and A-PPL (Azraoui, et al. 2015b). Enforcing access control was the sole reason for developing PPL (Sendor et al. 2011), which uses certified credentials before granting access. These credentials include attribute- and role-based access control (RBAC) systems (Ma et al. 2018), (Lebbat et al. 2016). The XACML PPL extension introduces a very effective means of enforcing rules; it uses the concept of obligations and a matching engine with a combination of a trigger and an action to execute the responsibilities relating to access control.

2.6.4.3 Geospatial XACML

The Geospatial eXtensible Access Control Markup Language (Poet 2014) extends XACML for declaring and enforcing access control policies that contain geometric and topological descriptions of the resources. The Adaptable and Programmable Policy Environment and Language (APPEL) (Herzog et al. 2007). The Platform for Privacy Preferences (M. Olurin, et al. 2012) has been developed as a W3C standard for expressing a web user's privacy preferences and data collection policies of a service provider. A preference/policy tells specific data items for which purpose they will be collected, who will receive the data and where the collected data be kept. The inability of the earlier languages such as XACML, GeoXACML APPEL, and P3P languages failed to satisfy the fundamental requirements for access control solutions, which are simple yet easy to use, leading to the development of the PrimeLife privacy policy language (Neven et al., 2010).

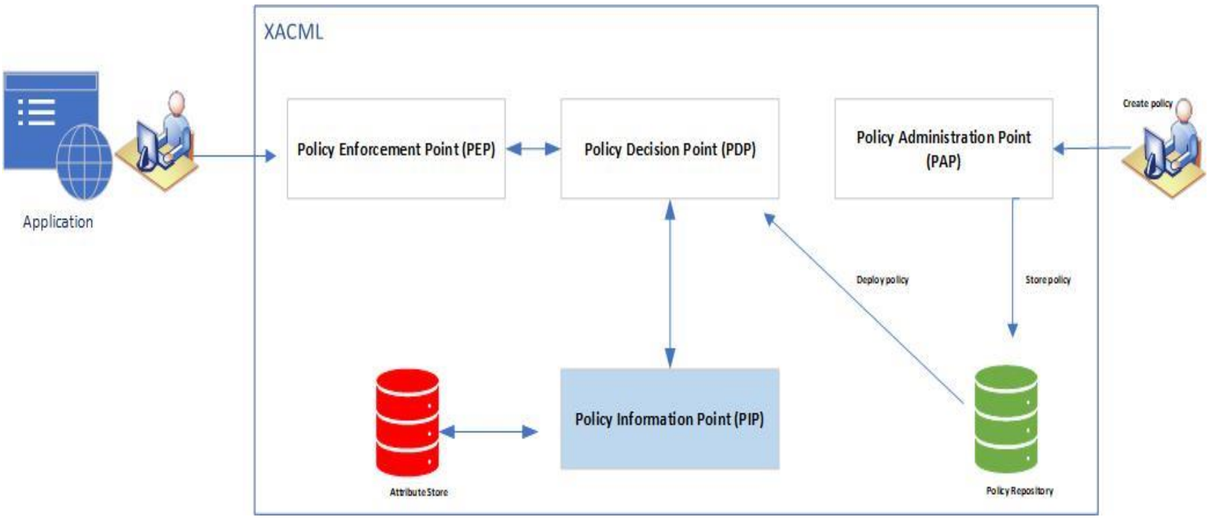

XACML
Application
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Policy Administration Point (PAP)
Create policy
Deploy policy
Store policy
Policy Information Point (PIP)
Attribute Store
Policy Repository

Figure 5: XACML (D. S. Kim, T. Shin et al. 2006)

2.6.4.4 Identity-based Authentication

Identity-based encryption authentication is a technique that relies on the public key. A generator is used to generate a Master public and Private key. The unique Master key is generated by relying on exclusive user data (Kumar 2019). Additionally, during decryption, a user obtains private access with his unique identity from a key generator to decrypt a file. The Private key has a dual role of both generating private keys and verifying the identities of users. However, trust issues arise with the Identity-based encryption authentication as the key generator holds both keys and is required to be actively online all the time.

2.6.4.5 Attribute-based Access Control (ABAC)

ABAC is a method for controlling access permissions. It is defined by policies that include attributes and results with different access rights levels for different users. The access policies are created using different types of attributes and enforced using the ABAC policies. The attributes that are considered include subject, environmental, resource, and object attributes. In the ABAC approach, the roles and rights of a user are prebuilt. The ABAC approach to solving security challenges, particularly authorisations, helps achieve efficient regulatory compliance with fewer complications at the implementation stage (Anand et al. 2018a).

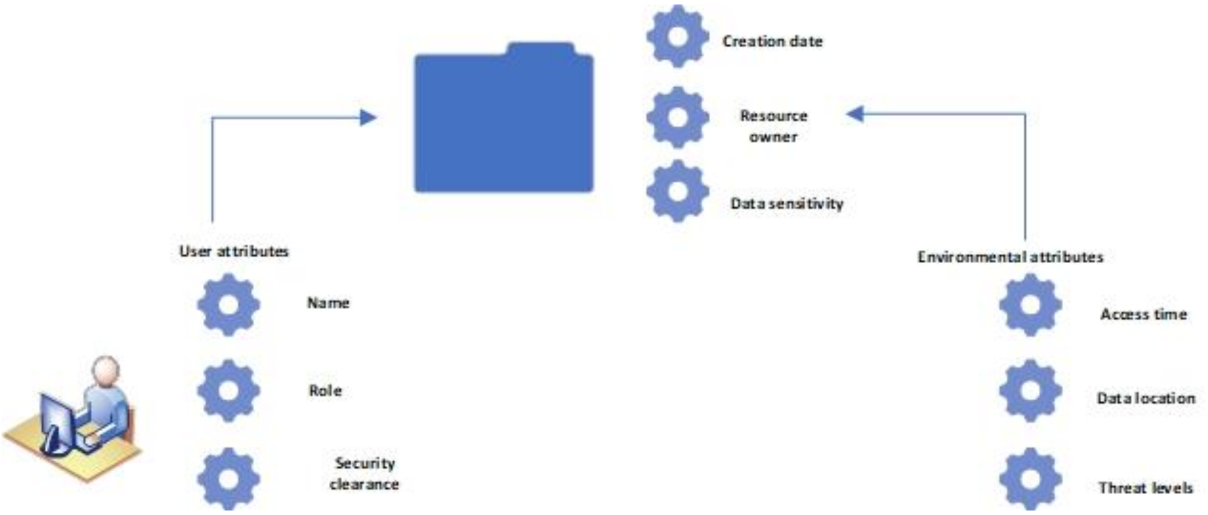


Figure 6: ABAC (M. Ed-Daibouni, A. Lebbat et al. 2016)

2.6.4.6 RBAC

RBAC is a framework that uses roles to control access to resources. Authorisations are grouped into a role, with the role having numerous members and a set of well-defined granular-level credentials. Under the RBAC scheme, access rights are provided based on users' roles and privileges. User permissions are given based on different parameters of RBAC, such as user roles, role permissions, and role relationships. The roles are classified into two categories: application/technical roles and organisational/business roles. The former roles contain a combination of different application-specific entitlement- or task-based permissions, and their scope is limited to the specific application. The latter roles are generated based on different job functions and access rights assigned to an employee (Zhu, et al. 2014).

The role-based authentication model requires the data owner to encrypt the hardware information and then upload the encrypted data to the cloud, such as blob storage in Azure. Reference (Rana et al. 2017) designed a role-based, AES based file encryption system. The scheme can be applied to all cloud models, including SaaS, and a one-time password is used to authenticate the users' additional security layers. The scheme is presented as a security solution for the whole cloud-computing environment, including SaaS contexts.

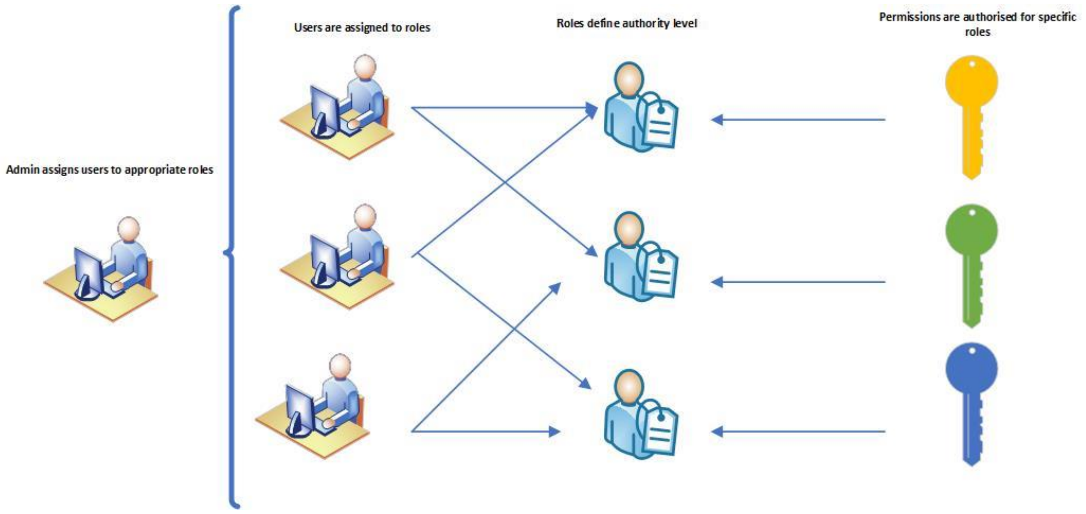

Admin assigns users to appropriate roles
Users are assigned to roles
Roles define authority level
Permissions are authorised for specific roles

Figure 7: RBAC(K. Soni, S. Kumar 2019)

The RBAC model accomplishes the two security systems principles: ‘least privilege’ and ‘segregation of duties. Recently, a substantial amount of effort has been spent using RBAC to support access control in systems. Though RBAC has its own set of limits, such as role explosion and role-permission explosion, it has been used to provide administration security in organisations with many users and permissions. In the RBAC scheme, there are mainly three rules for assigning permission to a particular user: role assignment, role authorisation, and permission authorisation. Permissions are provided to users based on these rules.

2.6.4.7 PPL

PPL (Sendor et al. 2011) was developed under PrimeLife project2 as an extension of XACML (OASIS, 2017) and similar languages such as P3P (M. Olurin, C. Adams et al. 2012). It allows for privacy-preserving access control using application-independent certified credentials for access authorisation based on credentials such as RBAC (Ma et al. 2018) and ABAC (Daibouni, et al. 2016). PPL also provides the benefit of regulating the use of personal information in secondary applications. It uses an obligation framework in the form of an application layer platform in a distributed-service-oriented environment to enforce the service provider's obligations or data controller to cater to a user or a data subject's privacy needs. This sets it apart from policy languages that came before it, which only provided minimal obligation capability and did not provide any concrete obligation specification model.

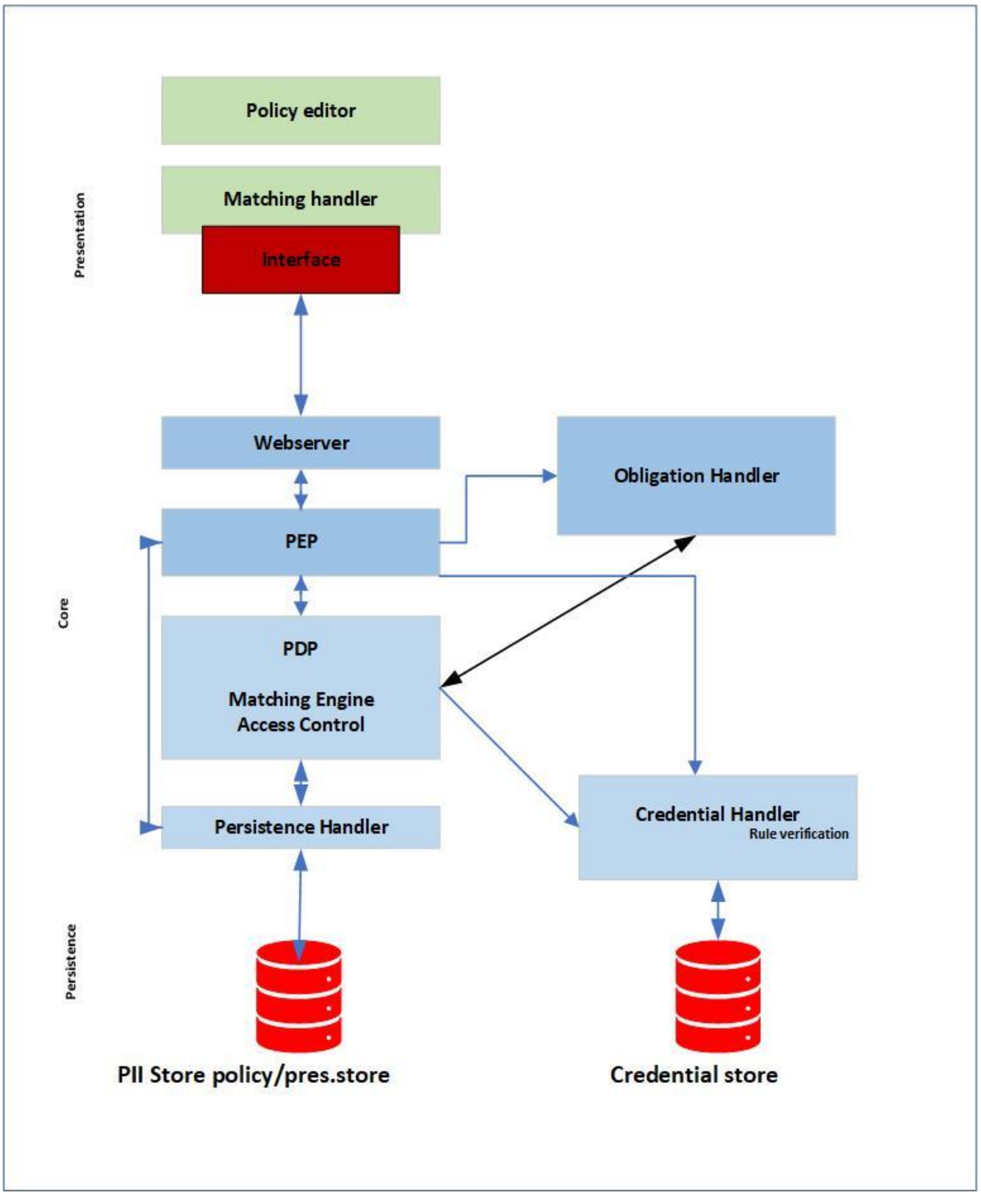


Figure 8: The PPL architecture (Curzon, et al. 2019, Enisa Europe 2019, Trabelsi, et al. 2011)

PPL's main contributions were in five main areas, including relying on two-sided data handling policies/preferences with automated matching and using credential-based access control to specify access control conditions in terms of the credentials that need to be presented. It also provided a form of equilibrium or symmetry by considering personal data as a particular type of resource in its own right. The PPL allowed for using the same language engine on the data subject’s side to describe access conditions before revealing data on the data controller’s side to specify which personal data need to be revealed to access which service and how those data will be treated.

Another significant contribution of PPL was the provision of a route for downstream usage of personal data. In this context, personal data became a resource the data controller offered to downstream data controllers or third parties based on the specifications the data subject or owner provided. Lastly, PPL contributed by adding event-based obligations to the initial XACML architecture. The obligation engine enforces this feature with the combination Trigger/Action, based on events attached to the execution of an obligation.

These XACML extensions were added to PPL to support all the above features in the local policies each of the entities expressed. PPL also defined some extensions to XACML used in the format to carry resource requests, policies, and credential proof statements from one entity to the other. However, as seen in recent extensions of PPL itself, there were limitations to the data subject's roles, the data controller, and downstream controller. PPL also did not incorporate accountability requirements as extended in the A-PPL and other recent extensions, such as the CPPL.

2.6.4.8 C2L

C2L aims at enforcing configurations that are permissible in a cloud environment (Poroor, 2012). The language uses spatio-temporal logic to express acceptable formats on colocations, hosting, security, and data migration. However, C2L only focuses on formalism and not real-life application in a live cloud environment. Similarly, Benghabrit *et al.* (2014) extended PPL and proposed an accountability framework to improve the safety and accountability of personal data handled by service providers.

Using an abstract policy language, they expressed the data subject's preferences and service provider's obligations in a human-readable fashion, thus achieving ease of mapping to the specification of policies (Benghabrit, et al. 2014).

Building on the PPL, Butin *et al.* (2013) proposed a privacy compliance solution for the satisfaction of accountability requirements in the cloud-focused on issues raised by how logs can be used for posterior compliance control. They presented real-world examples to demonstrate how to use log design for accountability and how it should be considered from the design stage. However, it works towards a formal verification framework.

2.6.4.9 Abstract Accountability Language (AAL)

Similarly, (Benghabrit, et al. 2014) extended the PPL Language and proposed a framework to deal with personal data in the cloud accountability and privacy issues to promote cloud services' safe use. They presented two different accountability policy languages; an abstract one devoted to the representation of preferences/obligations in a human-readable fashion, a concrete one for the mapping to concrete enforceable policies. They also validated their proposed framework solution with concrete use case scenarios. Their accountability policy representation framework enables accountability policy expression in a human-readable fashion using an abstract accountability language (AAL) (Grall et al. 2014). The framework applies the separation of concerns principle by separating the abstract language from the concrete one. They validated the ability of their framework to represent an accountability obligation in a health care use case. However, they were unable to implement it in a real-life scenario in any cloud computing model. The framework was auditor focused and therefore only extended the PPL with an Auditor role with corresponding Actions and Triggers to match corresponding obligations.

2.6.4.10 Accountability Privacy Policy Language (A-PPL)

The A-PPL (Azraoui, et al. 2015c) is a follow-up to (Grall et al. 2014) and an extension of PPL, which was designed to express machine-readable accountability policies instead of human-readable languages. A-PPL can define accountability and transparency rules on personal data handling using developed extensions of data retention, data location, logging, and notification.

This is done by introducing accountability rules, i.e., rules on data retention, data location, logging, and notification. Built on their previous works with (Benghabrit, et al. 2014) to develop a proof of concept focusing on accountability policies. They presented design requirements for the A-PPL with PPL extensions to handle accountability specific requirements such as notification, logging, and evidence collection. They also went further to describe an architecture of A-PPLE, the policy engine that enforces A-PPL policies. However, they have not provided any evidence of a finalised version of A-PPLE and how it works with any of the cloud Models like the SaaS for the enforcement of security and privacy obligations in an audit system.

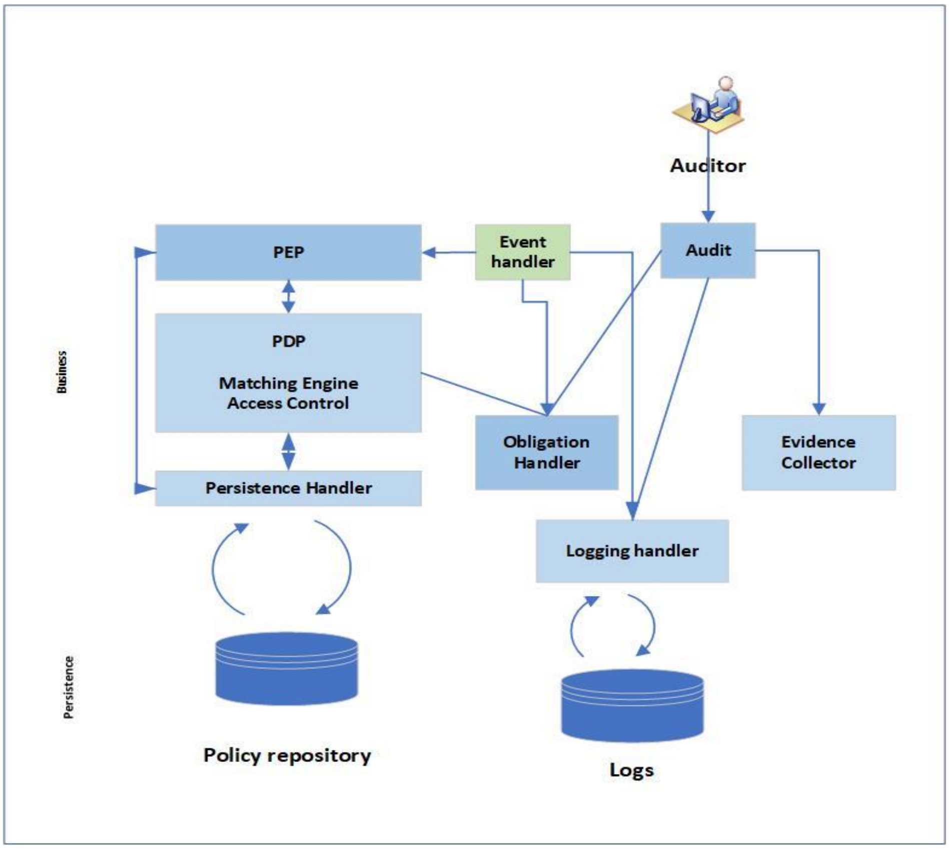


Figure 9: APPL (Azraoui, Elkhiyaoui et al. 2015b)

Vinh (2018) proposed a policy and architecture languages to specify and explain data protection properties in the policy and architecture levels. They built on previous works on the XACML, PPL, and A-PPL and demonstrated their expressive syntax and semantics by specifying a DPR policy and architecture for a smart metering service as a case study. The proposal expressed different variants of conformance relations between the defined architecture and policy. They proved and refuted using definitions, propositions and inference rules. Proposed policy language and architecture focused on expressing the design requirements button proposing a software tool based that can be experimented with in a real cloud environment. Unlike the A-PPL, it has not extended the PPL by adding additional data control roles, actions, and triggers. It is heavily mathematical with automated reasoning algorithms and, therefore, not combining the powerful combination of being human and machine-readable. However, it is one of its first semi-formal approaches to specify reasoning about data protection policies and architecture, particularly the GDPR.

2.6.4.11 Compact Privacy Policy Language (CPPL)

Another extension of PPL is CPPL (Henze, et al. 2016), which emphasises personal data privacy by compressing privacy policies using flexibly specialised domain knowledge. Butin, Paroor *et al.* (2013) Jayaraman (2012), (Benghabrit, et al. 2014), (Hiller et al. 2016, Azraoui, Elkhiyaoui et al. 2015c) contributed to an extended PPL, and (Jaatun, Pearson et al. 2016) presented a set of fundamental requirements that cloud providers or service providers must meet to satisfy the accountability requirements of their customers' data. They outlined several tools for an accountability-based approach, such as the Payment Card Industry Data Security Standard.

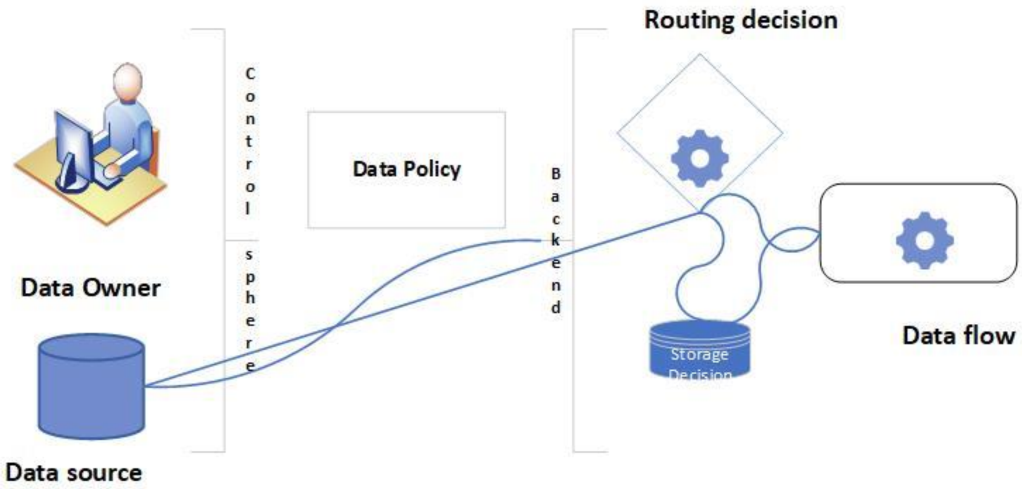


Figure 10: CPPL (Henze, Hiller et al. 2016)

2.6.4.12 PriArmor

PriArmor (Ghorbel et al. 2017) has been proposed to work with the IaaS model of the cloud. It allows data subjects to express their privacy preferences according to data protection regulations using an ontology model that includes all concepts of data access and usage within a distributed environment such as the cloud.

They added that their solution introduces a data flow model that tracks private data and reflects the existence of derived data through the system to maintain a healthy enforcement level and prevents data loss. The performed evaluation proves the efficiency of the approach to ensuring policy enforcement in the cloud environment. They instantiated and evaluated the enforcement infrastructure and the data flow model for the OpenBSD OS. Their work represents one of the most recent attempts at implementing privacy obligations in a live cloud environment with a specific cloud model, the IaaS. Their work purely focuses on the IaaS model of the cloud. They also have not experimented with the solution in a real-cloud-based environment.

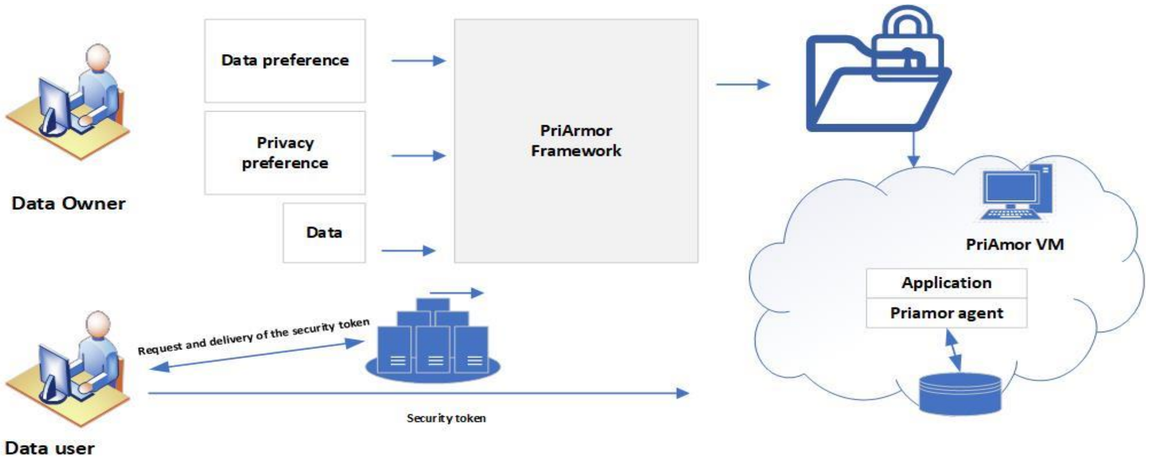


Figure 11: PriArmor (A. Ghorbel, M. Ghorbel et al. 2017)

2.7 Security, Privacy, and Data Protection Issues in SaaS Applications

In SaaS applications, data processing is carried out over telecommunications networks. The responsibility for ensuring security, privacy, and data protection primarily resides with SaaS service providers or is assumed to be shared with the user or organisation. This presents security, privacy, and data protection issues. To deliver a service or meet request, SaaS service providers may sometimes rely on outsourcing data handling and storage to third-party service providers, and these organisations or providers may rely on other service providers to handle the service or request.

Evidence abounds in the literature that security, privacy, and data protection challenges are hindering organisations' adoption of SaaS applications (Harikrishna, 2016). These challenges are the same ones organisations face in an on-premises setting, but they also include new challenges that emerge from the uniqueness of cloud technologies such as SaaS applications (Rashmi, et al., 2013).

Subashini, (2011), Rashmi, et al., (2013) argued that all aspects of an application delivery using SaaS must be secure. They listed the following core security elements that should be included in a SaaS application: data security, network security, data integrity, and data locality (Ambalkar et al. 2016). Other considerations include data access, data authorisation, data integrity, data availability, data privacy, data recovery, data authorisation, identity and authentication, virtualisation, and sign-on processes.

2.7.1 Location and Jurisdiction of Data

Without exception, data location is one of the most significant challenges SaaS applications face (Tiwari, 2014a). SaaS application data and the applications themselves are hosted on the service provider's infrastructure, posing several security and privacy challenges.

Georgios et al. (Stavrinides, 2017) argued that data-aware scheduling policies should be implemented to exploit data locality efficiently while considering the other characteristics of the workload and resource attributes. Accordingly, they investigated the impact of keeping data locally via simulation on SaaS applications performance in a real-time, data-intensive task are scheduled dynamically in numerous data availability conditions. According to (Kavitha 2011), a secure SaaS model must provide the customer's reliability on the consumer's data location. Abdullah et al. (2012) argued that the server's location where the user data resides is essential, and users should be assured that their service providers would not lose control over information relating to the location of their storage infrastructure.

Data protection regulations such as the GDPR require the location of data relating to EU citizens to be warehoused within the EU’s borders. This presents a significant compliance challenge to SaaS application providers and users alike.

2.7.2 Authentication and Authorisation Issues

Authentication and authorisation are described by Indu *et al* (2018a) as primary data protection issue in SaaS applications as SaaS applications services are hosted outside the corporate firewall. While authorisation is the method of permitting or disagreeing access to a particular resource depending on an authenticated user’s entitlements (Margulies 2015). Using authorisation mechanisms, the decision on which user is allowed to access or perform any action on the system and user identification information is used to decide whether to authorise access (Ethelbert, et al. 2017).

Barona et al., (2017) analysed diverse issues and threats relating to security, e.g., data breaches, undependable connectivity, resources sharing, accessibility, and insider attacks. They asserted that a breach relating to security and privacy might lead to unauthorized access and disclosure, unlawful destruction, and the modification of personal data transmitted, kept, or processed. Moreover, they examined data breach issues faced by SaaS applications and other cloud models. They further investigated difficulties presented by a breach and provided best practices to SaaS service providers.

Chen et al. (2008) investigated dynamic identity-based authentication schemes for use in an environment with multiple servers and how they can be used to enhance data security and privacy. Similarly, Hafizul *et al.* (2011) identified some authentication challenges and proposed an enhanced mutual authentication solution for remote users that relies on an identity-based cryptosystem. The solution ensures authentication by relying on a three-way handshake technique.

Subashini *et al.* (2011) considered other popular authentication technologies, including Security Assertion Markup Language (SAML) and Web Service (WS). SAML and WS Federation's substitute is a single sign-on solution deployed via a secured virtual private network tunnel. Tiwari *et al.* (2014) described authorisation as the mechanism defining the user's level of access. The SaaS service provider should have security capabilities and resources to check user authorisation and authenticate it using a secure mechanism.

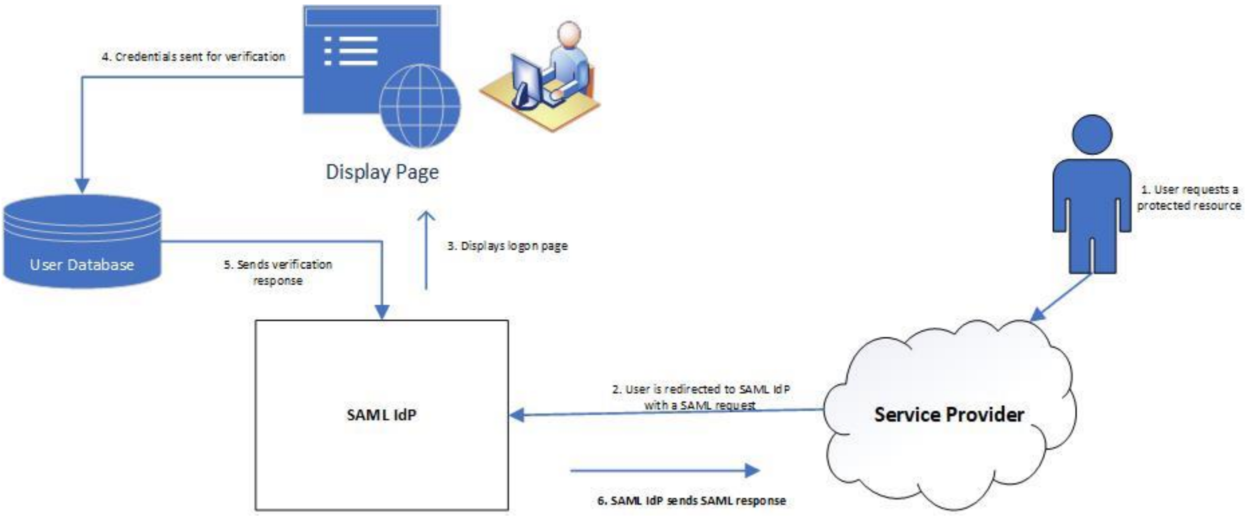

4. Credentials sent for verification
Display Page
User Database
5. Sends verification response
3. Displays logon page
1. User requests a protected resource
SAML IdP
2. User is redirected to SAML IdP with a SAML request
Service Provider
6. SAML IdP sends SAML response

Figure 12: SAML (CSA 2017)

2.7.1.1 Access Control

Authorisation in SaaS applications focuses on the application of access control models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC). Access control is central and a requirement to govern and protect data assets within an organisation (Uddin, et al. 2019) as security is the most crucial reason for organisations' disinclination to use the SaaS model. Access Control to web services and user data privacy preservation is the critical requirement for SaaS applications as SaaS applications hosted on the cloud is subject to unauthorised access and hence should satisfy proper access control model in these environments.

Guja et al. (2016) used ciphertext-policy attribute-based encryption scheme (CP-ABE) to protect stored data in disruption tolerant networks (DTN) as implementing CP-ABE onto DTN has some issues such as key escrow and attribute revocation. The CP-ABE is a variant of the ABE, and it associates a private key with a set of attributes and a ciphertext created with an access structure and is used to specify the encryption policy. Others are Hierarchical attribute-set-based encryption (HASBE) and multi-authority. Reference (Q. Zhang, S. Wang et al. 2019) utilized hierarchical identity-based encryption (HASBE) to provide ABE, ensuring data security while giving fine-grained data access. Conversely, (Xiong,et al. 2020) designed a multi-authority access control scheme for a cloud storage system and the internet of things (IoT) called SEM-ACSIT for secure access control.

2.7.1.2 Mandatory access control

Mandatory access control (MAC) mechanism is the traditional mechanism to define the access rights of users. MAC gives access permission through the operating system or security kernel. It controls data owners' ability to grant or deny access rights to clients for the file system. All-access control rights are set by the system manager and imposed by the security kernel or operating system (Jiang, 2016, Indu, Anand et al. 2018b).

2.7.1.3 Discretionary access control

Discretionary access control (DAC) is a security access control mechanism that controls the access permissions through data owner (Q. Dong, D. Huang et al. 2018). In DAC, each user's access rights are performed during authentication by validating the username and password. DACs are discretionary as the owner determines the privileges of access. In DAC, a file or data has an owner and the data owner controls the data access policies. DAC provides more flexibility than MAC; however, DAC provides less security than MAC (Wang, et al. 2016).

2.7.1.4 Task-based access control

Task-based access control is one of the many level access control mechanisms. Specific access permission is required for each task, action, or process represented by entitlement or task. This model can handle complex access conditions to determine whether the access rights need to be granted or denied. The entitlement access control model's primary concern is the maintenance of a large number of entitlement sets. Task-based access control model can represent and implement other hierarchical access control models like role-based access control and attribute-based access control. (Islam et al. 2019, Y. Liu, K. Xu et al. 2013)

2.7.3 Data Retention and Backup

Rajeswari *et al.* (2017) discussed critical challenges of data security in the cloud computing era. They argued that data privacy kept in the cloud infrastructure might be breached because of data owners’ inadequate security mechanisms. They analysed all categories and compared their strengths and weaknesses. Similarly, Takabi *et al.* (2010) described SaaS as a foundational model and evolving paradigm with unique features, which exacerbate security and privacy issues. They further explored the barriers to providing a dependable cloud computing setting. Mazahr *et al.* (2017) investigated many security challenges of SaaS and described data backup as an essential issue that needs to be carefully addressed.

2.7.4 Multi-tenancy and Data Segregation Issues

Tan *et al.* (2011) described a multi-tenant environment as having numerous users whose data are not visible or accessible to each other but can share resources or applications in an execution setting, even if they access the resources or applications from different locations and organisations. Multi-tenancy allows for optimal use of hardware and storage resources. SaaS providers should guarantee the distinct separation of data at the physical and application levels. Surya *et al.* (2013) described data segregation in SaaS applications as a situation where different users' data are hosted on the same data infrastructure. They emphasised that one user's data should not affect other users' conditions for accessing the same application in a multi-tenant environment. In some cases, this happens through malicious intent.

Furthermore, multi-tenancy presents substantial difficulties when deploying application components in the cloud because of varying isolation levels among tenants (Ochei, et al. 2015).

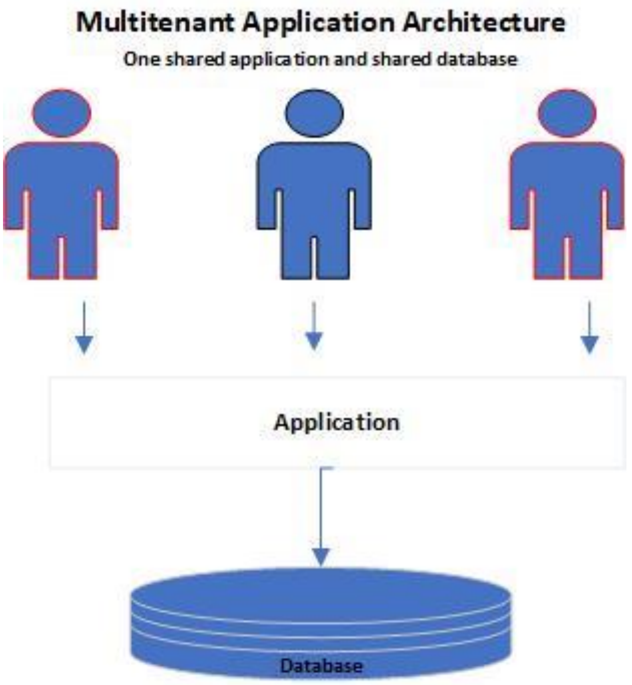

Multitenant Application Architecture
One shared application and shared database
Application
Database

Figure 13: Multi-tenancy; Ochei et al. (L. C. Ochei, J. M. Bass et al. 2015)

In some cases, this happens with malicious intents. Users' data must be segregated at the physical and application levels. Ochei *et al.* (2015) clarified that only authorised users have access to data in a multi-tenant environment.

2.7.5 Data Confidentiality

Data confidentiality is the protection of data from unlawful access, either intentional or unintentional. Per recent data protection regulations (e.g. the NDPR), users must be notified of any breach of personal data and protected from the breach. Kan *et al.* (2013) found that users store their data on cloud-based infrastructures, from where data can be accessed. As data outsourcing and portability increase, new security challenges are introduced, requiring auditing services or mechanisms to verify data integrity and privacy in the cloud. The authors proposed an efficient and secure dynamic auditing protocol to persuade users that data integrity can be guaranteed in the cloud. Additionally, Chen *et al.* (2015) highlighted the need for encrypting data before they are outsourced.

2.7.6 Data Availability Issues

SaaS providers are obligated to guarantee the availability of data without any disruption. Availability refers to a system's property being reachable and operational upon request by an authorized entity. The availability of a system comprises a system's capability to continue to operate even when some authorities are not functional. The system should be capable of continued operations even in the possibility of a security breach (Kulkarni, et al. 2013). Candan et al. (2009) explained that due to the associated cost of maintaining physical and software infrastructures, third-party service providers provide chargeable services for computation capability, storage, and connectivity to organizations

2.7.7 Data Integrity Issues

Data integrity is another critical element of a SaaS model. Tiwari et al. (Tiwari, 2014b) described data security and privacy as significant issues for SaaS application users due to their dependence on the cloud provider. They further argued that the SaaS service model provides many features, but adequate security remains a challenge. Further, they described existing solutions and proposed many SaaS security vulnerabilities and threats. Soni et al. (2017) analysed SaaS and cloud computing's security characteristics and data security concerns at large scales. They identified gaps and suggested future directions.

2.7.8 Network Security Issues

The network is the infrastructure for accessing SaaS application services. SaaS service providers must implement strict data protection measures to ensure that data are protected against manipulation, theft, and illicit access (Wang 2011b, Chouhan, Yao et al. 2015). Soni et al. (2012) proposed a Host Identity Protocol (HIP) because of the importance of the multi-tenant environment's security issues. Varadharajan et al. (2016)

described practices for spotting attacks such as virtual machines in a trusted virtual domain, in different domains, insider attacks, and attacks on services such as a database or domain name service (DNS), and web servers in a trusted domain.

2.7.9 Virtualisation

Virtualization is the process of extracting services, applications, computing resources, and operating systems from the hardware they run. The virtual machine and manager are the components that make up the concept of virtualization. Virtual machines are represented as an image, usually called the guest Operating System (OS) content memory and storage (Singh, 2017). It is an essential component of cloud technology. It works as middleware among servers and users and provides server virtualization, resource administration, data segregation, and multitenancy features. Jasti et al. (2010) described some threats such as insecure API's, unauthorized access, and malicious insider users related to the cloud-computing environment. Moreover, they evaluated security threats and explored how VM's can be exploited to access data and deny services, and they proposed helpful measures to avoid such occurrences.

2.7.9 Encryption

Minqh et al. (2010) claimed that unless security and privacy issues are tackled, the cloud's prosperity and SaaS will be slowed. They presented many barriers, including encryption that is slowing the adaptation into the SaaS applications. Naemu et al. (2017) reviewed the benefits of virtualization and its cost-effectiveness and proposed a novel security architecture to protect warehoused VM images in clouds via encryption, decryption Kerberos. Banirostom et al. (2013) also reviewed and proposed a new approach to improve data encryption and integrity. They called it Trusted Cloud-Computing Infrastructure. Kavitha (2011) and Rashmi,

(2013) further proposed that SaaS vendors must ensure that critical aspects are covered across layers to ensure data security.

2.7.10 Standardisation and Interoperability

According to Majda *et al.* (2015), interoperability is the property of a user solution whose interfaces can fully understand and work with another service provider’s system in the present or future, with restricted access. Rafael *et al.* (2013) described service movability among diverse cloud service providers as challenging because of a lack of standard interfaces for interrelating with other service providers, services, and formats for managing virtual appliances. Therefore, there is no standard interfacing with a SaaS application service provider, and each service provider has its API. Rashmi *et al.* (2013) discussed how to achieve interoperability among cloud services, including SaaS applications, and improve their steadiness, privacy, and security. Therefore, standards are desired from a diverse set of organisations responsible for standardisation such as the ISO or the Cloud security alliance (Sahoo, 2013).

2.8 Chapter Summary and Conclusion

This chapter highlighted some of the fundamentals of SaaS applications, discussed the concept of privacy, and established a link between SaaS applications, privacy, and data privacy. The chapter also discussed the concept of data protection, including data regulations such as the NDPR and GDPR. Furthermore, privacy and data protection issues were discussed in detail, and finally, compliance with data protection regulations was discussed in SaaS applications. Issues relating to privacy and data protection can hinder SaaS applications' adoption, such as compliance with data protection regulations. The knowledge gained in this literature review of SaaS applications, privacy, and data protection has been used to refine the research and enrich the methodology design, data analysis, requirements identification, and subsequent design of a policy language to specify and express the compliance requirements of data protection regulations at every stage of a data life cycle (Gjermundrød, Dionysiou et al. 2016).

CHAPTER THREE

3.0 Methodology and Approach

3.1 Introduction

In the previous chapter, the literature revealed a diverse number of use cases, fundamentals of SaaS applications and discussed the concept of privacy. The Chapter revealed a link between SaaS applications, privacy, and data protection within the context of the research. Further, the chapter explains the purpose and rationale for the research methodology adopted in this research work. An analysis of the relevant methods used within the context of ensuring privacy, data protection, security and the design or an artefact justifies both the appropriateness of the methodology and their limitations is presented.

3.1.2 Purpose

The purpose of this Chapter is to provide an overview of the research methods chosen and describing how these methods have been adopted in this research, and further discussing their suitability within this domain and their limitations. Additionally, the chapter discusses ethics, data collection, analysis, and evaluation, as well as case study.

3.1.3 Structure

Section 3.2 starts by restating the study goals and the methods used to accomplish them. Section 3.3 discusses the research methodologies used to gather data relevant to the study environment, emphasising a combination of design science research and semi-formal procedures that included a survey and focus group session. Additionally, the Chapter includes sections on the rationale and strategy in sub-sections 3.3.1 and 3.3.2, where ethical aspects are examined. Sections 3.4 and 3.5 discussed design science theories and strategies. In 3.6, semi-formal approaches were discussed; in 3.7, a preliminary study methodology was adopted; and in 3.8, the Chapter summary was offered.

3.2 Selecting Research Methods

As stated in Section 1.3, the overall aim of the research is to design an extended, semi-formal policy language for privacy and data protection compliance for SaaS business applications by expressing requirements for a) the privacy of personal data and b) the achievement of compliance with data protection regulations that relate to the privacy of personal data.

The objective is to determine if privacy, security and data protection issues in SaaS applications adoption are inhibiting adoption. In order to meet the aim of the research for example, there is then a need use appropriate methods to establish if a means of compliance can help achieve compliance with privacy and data protection regulations by organisations. Therefore, the research was conducted by selecting two techniques of qualitative research methods at the preliminary stage of the research and in the second stage, by relying on the design science strategies and a semi-formal method to design the artefact.

3.3 Research Methods – Design Science and Semi-formal Approach

The thesis is rooted on cloud computing technology and the regulatory realms of privacy and data protection. Cloud computing technology research is often classified as computer science, but privacy and regulatory difficulties are classified as social and legal challenges, but have evolved from a variety of areas, including technology, psychology, and mathematics. Both areas share a dependence on an adequately developed research approach based on a variety of inquiry tactics, including qualitative, design science, semi-formal methods and mixed methods (Creswell 2003).

As indicated in Section 3.2, the study relies on the combination of the design science and semi-formal methods (Hevner, Chatterjee 2010a), (Bj\orner, Havelund 2014). Therefore, the methodological approach is a blend of approaches covering two stages of the research: a preliminary stage, where relevant data was collected using questionnaires and a focus group session held in Nigeria and the policy language design stage where semi-formal notations were used to design the specification language, SaaS-PPL artefact.

3.3.1 Rationale and Approach

A research methodology underpins a research process that places philosophical values and assumptions at the heart of the research, guiding how data is applied to arrive at conclusions (Kumar 2018). Furthermore, a research methodology employs a scientific approach to help address the research objectives. It is often the case that those who apply design science and semi-formal approaches are practitioners, that is, academics who have been invited to proffer a solution to an existing problem (Wieringa 2014).

The research methodology used in the current research is a combination of design science methods (Kogan, Mayhew et al. 2019) and semi-formal methods. The aim is to design a new artefact - a semi-formal policy language to specification security, privacy, and data protection regulation properties. Although the design science method entails applying knowledge derived from everyday organisational operations to problems, it also involves discovering and applying new knowledge to previously unsolved challenges (Wieringa 2014).

Historically, research design has been applied to all disciplines, including engineering, technology, architecture, and the arts. Designs are fundamental to almost all professions (Wieringa 2014). Design and semi-formal methods are highly relevant because they address the issues of outputs such as artefacts.

Semi-formal methods (Bj\orner, Havelund 2014) refer to principles of selecting and applying techniques and creating artefacts. Thus, code designs, program designs, or software or systems components are considered mathematical artefacts. This research shall consider design science methods and semi-formal methods, techniques and strategies.

3.3.2 Ethical Considerations

There are numerous statements of ethical practices that research bodies and professional bodies have devised, such as the ACM and British Psychology Society. Bromley, et al. (2015) identify four main areas whether there is harm to participants, whether there is lack of informed consent, whether there is an invasion of privacy; whether deception is involved;

Harm, in the context of this research, relates to the effect any of the use of the data may have on the participants. Therefore, it would be unethical to design a study that the outcome may harm any of the participants respondents or violate their privacy.

3.4 Design Science

Design science was identified as a suitable approach to this study because it provides a rigorous process for designing and evaluating artefacts that solve observed problems, communicating the results to various audiences, and contributing to research (Weber 2011). The utility of the system and the characteristics of the organisation and implementation methodologies together determine the extent to which that purpose is achieved (Hevner, Chatterjee 2010b).

Design science is fundamentally a problem seeking paradigm, and it aims to create an innovation that defines the ideas practise technical capabilities and product through which the analysis, design, implementation and the use of an information system can be effectively and efficiently accomplished (Orlikowski & Iacono, 2001). Design science is vital for a discipline-oriented to watch the creation of successful artefacts.

For some researchers, it is not enough to study and understand why nature is as it is; they want to know how they can improve it (Cross, 2001). Design science research attempts to focus human creativity into the design and construction of artefacts not have utility in application environments (Hevner, Chatterjee 2010b)

Table 3: Examples of Design Science Studies

No.	Authors	Theories Used	Artefact Developed
1.	(Li, Werner et al. 2020)	Hevner and Chatterjee (2010);	
2	(Brodin 2019a)	Hevner and Chatterjee (2010); (Gregor and Hevner (2013)	GDPR compliance framework
3.	Barafort et al. (2018)	Design Science Hevner	TIPA Framework
4.	Bragge, Tuunanen, Virtanen, & Svahn (2011)	Design Science-Hevner	A repeatable collaborative technique for establishing new technological value systems
5.	Levermore, Babin, & Hsu (2010)	Design Science- Hevener	Artefact that combines matchmaking with global database query
6.	Mueller & Strohmeier (2010)	Theory of Information System	A virtual learning environment for business training and development
7.	Adomavicious, Bockstedt, Gupta, & Kauffman (2008)	Process Theory – Design Science Approach	IT Ecosystem Model – IT development patterns may be studied using a formal issue representation framework.
8.	Jiang & Benbasat (2004)	Design Science- Hevener	Virtual Product Experience – a tool that lets users edit online photos and examine them from various viewpoints
9.	Novak, Hoffman, & Yung	Hoffman and Novak (2000)	A structural Model – to assess a customer's online experience

3.4.1 Theories in Design Science

Theories are critical in both the scientific and social sciences. The natural sciences have progressed mainly via intensive theory creation and testing using positivist techniques. The creation and testing of theory have aided the social and behavioural sciences (Venable, 2006).

However, Herbert Simon (1996) highlighted the necessity for design sciences. Design science is a problem-solving activity that uses emerging technology as the main product. (Simon 1996). A design in information science provides instructions or concepts for implementation since design theories are prescriptive, unlike explanatory and predictive theories in the scientific and physical sciences.

The IS community uses design ideas to enhance the efficacy and usefulness of IT artefacts in addressing real-world business issues (Hevner & Chatterjee, 2010) Table 2.6 includes design science scholars' design theories.

Table 4: Design Theories in Information science (IS) research

Study	Process
Nunamaker et al. (1991)	The process comprises of five stages: 1. Construct a conceptual framework 2. Develop a system architecture 3. Analyse and design the system 4. Build the (prototype) system and 5. Observe and evaluate the system.
Walls et al (1992)	Addresses both product and process design. Four components about the design product: 1. Meta-requirements 2. Meta-design 3. Kernel theories and 4. Testable design product hypothesis Three components about the design process: 5. Design method 6. Kernel theories, and 7. Testable design process hypothesis Kernel theories are drawn from natural or social sciences, as above, but apply to the design method.
March & Smith (1995)	Design activity consists of: 1. Build 2. Evaluate 3. Theorise 4. Justify

Hevner et al. (2004)	Seven guidelines for Design Science in IS research: 1. Design as an artefact 2. Problem Relevance 3. Design evaluation 4. Research Contributions 5. Research Rigour 6. Design as a Search Process 7. Communication of the Research
Venable (2006)	1. Solution technology investigation 2. Theory building 3. Artificial evaluation 4. Naturalistic evaluation
Gregor & Jones (2007)	1. The purpose and scope 2. Constructs 3. Principles of form and functions 4. Artefact mutability 5. Testable propositions 6. Justificatory knowledge 7. Principles of implementation 8. Expository instantiation

These approaches are described in many ways in the design theories literature, such as constructive design (Livari et al. 1998), system development (Gregor & Jones, 2007), and design science (Hevner, Chatterjee 2010b)

These design theories all concentrate on how an object can be created by relying on a development process and appearing when produced based on specific design principles. Prescriptive statements are an actual product of design science research, according to most publications discussing theory. It is helpful to compare design science's viewpoint with that of design. The former provides guidelines for practice, guaranteeing that professionals and other design science researchers can understand concepts. Science requires theorising and building theories. In comparison, design theories aid designers in creating successful products (Lukyanenko, Parsons 2013). This section will discuss some of these theories in more detail.

3.4.1.1 Gestalt Theory of Design

In the 1920s, Germany pioneered the study of gestalt. A significant portion of the theory is based on psychological and cognitive processes.

"Gestalt" refers to a unified physical, psychological, or symbolic structure with characteristics that cannot be deduced from its constituents (Courtright, 2002).

These theories explain how individuals prefer to organise visual components into groups or unified wholes when specific rules are followed. These are the principles of analogy, continuity, closure, proximity, figure, and ground. (Moore & Fits, 1993). Gestalt theory examines how we perceive our surroundings. It explores different concepts that assist us to determine which is figure and ground (Courtright, 2002).

3.4.1.2 Classic design theory

Design is creating and arranging pictures to convey a message, viewpoint, emotion, concept, or idea. It uses icons, drawings, colour, lines, forms, textures, and hues (Johnson, 2008). A classic design has remained timeless. The majority of traditional designs are uncomplicated and straightforward. This concept summarises the components of design, including line, form, space, structure, value, and colour, and the design guidelines of movement, emphasis, harmony, and harmony (Lauer, Pentak 2011). The classic theory of design asserts that a designer's work is pleasant to spectators or viewers due to how the design components are arranged in line with design principles. This idea has survived for thousands of years and has no single source of origin

3.4.1.3 Pattern Theory

Pattern theory, promoted by Ulf Grenander in the 1970s, is a mathematical framework to explain knowledge in terms of patterns. It theoretically framed many concepts, methods, and findings from computer vision, voice recognition, pattern recognition, image processing, and artificial intelligence Knill & Richards, (1996).

The software world adopted the pattern vision because it addressed long-standing issues in software design in general and object-oriented design in particular. Pattern theory has been one of the most frequently utilised and significant software architecture and design concepts in the last decade (Alexander, 1999).

3.4.1.4 Cognitive Load Theory (CLT)

CLT began in the 1980s and was further expanded in the 1990s by scholars worldwide (Paas et al., 2003). CLT is a psychological theory that tries to explain human behaviour by studying our thoughts as humans are assumed to be rational creatures who make rational decisions. The goal of CLT is to help instructional designers decrease the burden imposed by poorly designed learning materials (Cooper, 1998). The CLT involves working memory, long-term memory, and sensory memory (Pass et al., 2003)

3.5 Design Science Strategies and Steps

According to (Mullarkey, Hevner 2019, Hevner, Chatterjee 2010a), design science includes a set of strategies required for conducting and evaluating design science research. These strategies are further explained in Table 3.

Table 5: Strategies for executing design science research

Step 1: Artefact design, usually referred to as ‘design as an artefact.’	In design science, a viable artefact should always be designed as an outcome of the research.
Step 2: Problem significance or relevance	The design science approach’s sole intention should be to create or develop a technology-based solution that has relevance to an existing problem or challenge organisations face.

Step 3: Design evaluation	The utility of the artefact must be demonstrated by relying on a well-executed evaluation method.
Step 4: Research contribution	Design research should show clear evidence of its contributions.
Step 5: Rigour of the research	Research conducted using the design research methodology must rely on applying methods adjudged to be rigorous in the execution and evaluation of artefacts.
Step 6: Design as a search process	The design as a search process stage of the design science method requires reviewing the current state of the art and identifying gaps in the literature.
Step 7: Communication of the research	Under the design research methodology, the outcomes of the research must be communicated to relevant audiences.

(Source: Hevner *et al.* (2010) (Hevner, Chatterjee 2010a), Mullerkey *et al.* (2019) (Mullarkey, Hevner 2019))

According to Mullarkey *et al.* (Mullarkey, Hevner 2019), there must be evidence of clear research contributions in designing an artefact and the evaluation of methodologies. Researchers must use their research skills and academic judgments to determine how to apply guidelines or strategies for conducting design science research. Additionally, the authors argued that each of these seven strategies must be executed to complement the design science research methodology. The seven strategies are explained in more detail below.

3.5.1 Step 1: Design as an Artefact

The designs developed in this thesis are based on the production of specific artefacts in the form of a semi-formal policy language with an extended syntax and semantics. The SaaS-PPL policy language extension provides an approach (method) and syntax (model) to capture the privacy and data protection requirements of the NDPR at multiple levels of abstraction.

The outcome of any design research is a design that is more focused on serving an organisational need. It must be defined or described effectively to be implemented and applied in an appropriate setting. According to Riemer (2014) (Riemer, Johnston 2014), artefacts are fundamental to information and computer sciences. Consequently, they are considered to be interdependent with the contexts of their application.

In the current research, the artefact produced is a language specification expressing security, privacy, and data protection properties of SaaS business applications. The artefact is created by relying on semi-formal methods to develop the extended syntax and semantics of PPL and express the security, privacy, and data protection properties of the NDPR. The artefact serves three groups: software developers, data compliance managers and management. The SaaS-PPL work is detailed in Chapter 6.

3.5.2 Step 2: Problem Relevance

The literature review in Chapter 2 identified the relative shortage of mechanisms and techniques for assessing and improving compliance with relevant regulations such as the NDPR. Additionally, although SaaS-PPL is particularly suited to capture SaaS applications' compliance requirements, it is not suited for capturing business process properties. Thus, to be relevant in the business process domain, the SaaS-PPL policy language will require further standard extensions.

Compliance with security, privacy, and data protection regulations remains a significant problem across all sectors and industries. Based on the evidence in the literature review, there are no existing methods or mechanisms to ensure compliance with the data protection requirements of the NDPR the government in Nigeria has enacted, which now poses a significant problem for organisations. Thus, confirming the problem relevance as governments and regional bodies continue to enact data protection laws such as the NDPR (Tamburri, 2019), the GDPR, (NDPR, 2019), and California Consumer Protection (CCP) Act, 2020 (W. Stallings 2020a).

Furthermore, in the early part of the research process, the researcher conducted a focus group session and collected data from specific high-profile organisations in Nigeria to understand their concerns about security, privacy, and data protection in SaaS applications. The justification behind using a questionnaire survey and a focus group session was to triangulate data and find consistencies and reoccurring themes in the data (Wray, Markovic et al. 2007).

3.5.3 Step 3: Design Evaluation

The value and utility of a design artefact must be supported using an evaluation method. As (Hevner, Chatterjee 2010a) noted, evaluation is a critical element of the research process. The proposed policy language artefacts such as syntax and semantics extensions have been designed and validated in a case study using semi-formal proofs. These proofs have shown matching of the specified properties of compliances with privacy and data protection properties. This outcome is described in Chapter 7 using a scenario that demonstrates the utility of the policy language.

Furthermore, an artefact is said to be complete when it has met all requirements and when it is regarded to be fit for the purposes for which it was designed. In the design science method, artefacts can be evaluated using several design science techniques, including observation, analytical, experimental, testing, and descriptive techniques.

In addition to the design science evaluation methods, in this research, a combination of (Hevner, Chatterjee 2010a) observation techniques using a case study scenario and Bjorn’s (Bj\orner, Havelund 2014) semi-formal proof techniques is employed. Semi-formal methods use mathematical proofs to evaluate and confirm correctness (Gawanmeh, Alomari 2015).

The evaluation aims to determine whether the syntax and semantics of the new policy language have specified the service provider obligations and user preferences correctly based on the data protection regulation's properties. Details of the semi-formal proofs of the evaluation are provided in Chapter 6.

3.5.4 Step 4: Research Contribution

Hevner (Hevner, Chatterjee 2010a) argued that the eventual assessment of any research project requires the ability to answer the research contributions' question. This research study contributes to the design of a specification language as described by Bjorn *et al.* (Bj\orner, Havelund 2014), such as the extension of PPL into an artefact called the SaaS-PPL specification language, a set of obligations, policies; syntax and semantics extensions; and the mapping of privacy and data protection requirements of the NDPR. Full details are provided in Chapter 6.

This study also evaluates the compliance check syntax to show evidence of compliance with the NDPR regulation as a contribution by matching and evaluating service provider obligation, user preferences, and privacy and data protection regulation properties.

3.5.5 Step 5: Research Rigour

The research rigour strategy of the design research methodology relates to how the research is carried out. In the design research methodology, rigorous methods are applied to designing, building, and evaluating the artefact. Any academic exercise or endeavour’s rigour is derived from the practical application and use of existing theoretical foundations and proven methodologies.

Therefore, a research study's success will depend on the researcher's ability to select the most appropriate techniques for designing and evaluating the artefact.

SaaS-PPL is based on PPL, which is designed for access and authorisation. SaaS-PPL extends PPL to adapt to new privacy and data protection regulations, such as the NDPR and GDPR, based on semi-formal methods and accepted standards for system specification. SaaS-PPL extends PPL with syntax and semantics for the entire data life cycle, including collecting, processing, storing, retaining, and forwarding. The addition of semantics is based on existing policy language arrangements.

This research study has foundations in computer science, law, information science, privacy, and data protection principles.

The SaaS-PPL artefact presented in the research was designed after a thorough review of the literature and the gaps in existing approaches to compliance (see Section 2.0), including the justification of the need to using formal and semi-formal methods to design the artefact based on semi-formal techniques (see Section 6.0). Additionally, the SaaS-PPL artefact was rigorously evaluated using an NDPR case study.

3.5.6 Step 6: Design as a Search Process

The SaaS-PPL design is founded on reviewing the gaps identified in the current state of privacy, security, and data protection in SaaS applications (see Chapter 2). After the initial PPL version was published, the language was extended and refined over several iterations that added support for the specifications of privacy, security, and data protection regulation requirements in different contexts.

In design science research, the search process represents discovering a solution to an existing problem. Additionally, the process of solving a problem can be described as applying available resources to arrive at the desired end while following existing regulations or limits imposed by the environment.

3.5.7 Step 7: Communication of Research

SaaS-PPL is presented from a technical viewpoint and directed at data protection managers and developers. Although higher-level motivations of managerial audiences are discussed to some degree, they are not the focus. However, the broader scope of the thesis will address concerns of managerial audiences as well.

Stakeholders with technical backgrounds need sufficient detail to create the described artefact, whereas administrative audiences need sufficient detail to decide whether it is necessary to integrate the described artefact into the organisation’s overall plan. Design science studies must be evidence-based and simplified to cater to diverse stakeholders Hevner *et al.*, (2010a). Furthermore, the research communicates and demonstrates the numerous benefits of SaaS-PPL language to organisations concerning the specification of their privacy and data protection compliance requirements as required by data protection regulations. In the following section, the design evaluation approach of the design science methodology is discussed.

3.5.8 Design Science Evaluation Techniques

After an artefact is designed, it needs to be evaluated. The researcher relies on semi-formal methods and the mathematical proof system to evaluate the artefact’s properties and notations. The case study context supports this approach. The proof system evaluates personal data properties at each level of the data life cycle and matches them against the service provider’s sub-policies and obligations specifications and the user’s data handling preferences.

The mathematical proof system showed how all the properties complied with data protection regulation provisions such as the NDPR.

Full details of the case study are presented in Section 7. Hevner *et al.* (2019) identified five distinct evaluation techniques: observational, analytical, experimental, testing, and descriptive.

Accordingly, in this research study, a combination of semi-formal proofs and observational case study evaluation techniques is used to appraise and evaluate the artefact. These techniques are well suited for this research because the semi-formal proof technique evaluates the artefact, and the case study puts it into context and provides insights into how the artefact can be applied to a particular setting. The case study's primary purpose is to investigate the regulatory, economic, technological, and social contexts of a case.

3.6 Semi-formal Methods

According to (Bj\orner, Havelund 2014), a semi-formal method describes its techniques and tools using mathematics and other modelling tools such as the unified modelling language (UML). For example, if the method includes a specification language, it must have a semi-formal syntax, semantics, and a proof system developed according to established standards. Semi-formal methods can help construct a specification and analyse, transform, or refine existing or pre-existing specifications. Besides being employed to design specification languages for software packages, formal methods are used for developing software requirements (Souri, et al. 2018).

The aim of using semi-formal software development methods is to reason about and determine the properties of the software or application under development (Ed-Daibouni, et al. 2016). These properties may include the correctness of a program code regarding the system's requirements and other resources such as computing usage. For this research, the specification language will be the focus.

3.6.1 Specification Language

Specification approaches or methods are believed to have been early types of semi-formal methods. Some early semi-formal specification languages include Z (Saratha, Uma et al. 2017, O'Regan 2017), RAISE, RSL (Bjørner, Henson 2007), and VDM (Larsen, Lausdahl et al. 2010). These specification languages aim to build and specify readable expressive program requirements, syntax, and semantics. Therefore, the major challenge of writing simple-to-comprehend specifications alongside evaluation and analysis tools remains (Navimipour 2015).

3.6.2 Syntax and Semantics

3.6.2.1 Syntax

Syntax is a form of expression, a statement, and a program unit. Additionally, the syntax is used in a language or program to signify the language or program's structure but not it's meaning. A language's syntax is a collection of rules that validate the sequence of symbols and instructions used in a language or program (Alves-Foss 1999).

3.6.2.2 Semantics

According to Gawanmeh and Amjad (Gawanmeh, Alomari 2015), a language's semantics clarifies the meanings of expressions, statements, and program units. It is used to understand the relationship between syntax and the model of computation of a language or program. Semantics emphasises the interpretation of a program to understand it easily or predict the outcome of the program's execution. Schobbens and Yves (Schobbens, Heymans et al. 2006) contended that a language is not fully defined without formal semantics.

3.6.3 Semi-Formal Proof System

Semi-formal mathematical proofs should be presented in a way that is easily comprehensible to mathematicians. A semi-formal proof is proof that every logical inference has been checked, going back to mathematics' fundamental axioms. All the intermediate logical steps are supplied, without exception. No appeal is made to intuition, even if the translation from intuition to logic is routine. Thus, a semi-formal proof is less intuitive and yet less susceptible to logical errors (Souaf, Berthomé et al. 2018, Hales 2008a).

In the following sections, the researcher describes the data collection methods executed at the preliminary investigation stage.

3.7 Preliminary Investigation

In the preliminary part of the research, the researcher collected data from a select number of organisations in Nigeria to meet the initial stages of the research and answer the research questions. Along with primary data, the researcher extracted requirement data from relevant data protection regulations based on privacy principles by design (Cavoukian 2020).

Because this research involves human respondents, ethical concerns were addressed. The greatest care was taken to recognise and comply with regulations concerning the ethics of research conduct. All regulations, policies, and standards relating to ethics set by the University of Central Lancashire (UCLAN) were strictly adhered to.

The principles of professional integrity, confidentiality, and personal privacy provided by the GDPR were considered throughout the research study. Consent of all participants was obtained before the focus group session and a questionnaire survey were conducted. An information sheet, approved by UCLAN, was provided to all participants and their organisations before participating in the research study.

3.7.1 Data Collection Methods

Qualitative data are collected for the sole purpose of analysing the problem the targeted audience faces and providing clarity on the impact of the problem on the targeted audience (Pat Bazeley and Kristi Jackson 2013). Several types of qualitative data-gathering techniques exist, including focus groups, in-depth interviews, and observations (M. M. Krupp, M. Rueben et al. 2017). Three of them will be compared to determine the relevance of these techniques to the current research work.

Generally, qualitative data-gathering tools are all useful; however, their suitability depends on the research questions, needs, and goals. In this research, a focus group session and questionnaires were employed in the early stages to engage with relevant organisations in Nigeria. Because of the sensitivity of privacy and data protection issues, many participants data were anonymised and relevant consents collected after administering participant information sheets.

3.7.1.1 Questionnaire

A questionnaire is the main means of collecting quantitative primary data (Roopa, Rani 2012). A questionnaire enables quantitative data to be collected in a standardized way so that the data are internally consistent and coherent for analysis (Kazi, Khalid 2012). Questionnaires should always have a definite purpose that is related to the objectives of the research, and it needs to be clear from the outset how the findings will be used.

A questionnaire is used in case resources are limited as a questionnaire can be quite inexpensive to design and administer and time is an important resource which a questionnaire consumes to its maximum extent, protection of the privacy of the participants as participants will respond honestly only if their identity is hidden and confidentiality is maintained, and corroborating with other findings as questionnaires can be useful confirmation tools when corroborated with other studies that have resources to pursue other data collection strategies (Chong, Diamantopoulos 2020).

3.7.1.2 Purpose of the Questionnaire

The purpose of this survey is to capture the privacy, security and compliance with data protection regulation concerns of organisations relating to SaaS applications and data protection in the retail sector in Nigeria. The results of the survey are intended for requirements gathering towards the designing a novel privacy and security compliance mechanism or tool for SaaS business applications.

The questionnaires were deployed after obtaining ethical approval from the university. The data collected from the questionnaires were intended to be used for designing a privacy and data compliance mechanism for SaaS applications. The researcher used the university's Microsoft Forms tool for data collection. This satisfied the university's data handling policies and complied with the EU's new GDPR. The questionnaires targeted participants in highly strategic organisations in Nigeria.

3.7.**1.**3 **Focus Group**

A focus group is a group interview involving a small number of demographically similar people or participants who have other common traits or experiences. Their reactions to specific researcher posed questions are studied (Hasni,et al. 2020).

In the first stage, the focus group technique has been selected regardless of other qualitative research methods mainly due to its ability to allow researchers to ask questions, and to instigate clarifications of ideas by allowing direct communications between participants during the session (Satrjeenpong, et al. 2018) To determine the success of this technique, a moderator (or a moderating team) must be chosen to lead the discussion by asking the participants open-ended questions on a specific topic of interest. In addition to leading the discussion, the moderator also plays an important role in creating a comfortable environment for the participants, thus promoting more “natural” conversation between them - without heavily relying on the questions from the moderator (Moudra, et al. 2020). In general, focus group works predominantly quite well especially for the pilot testing proposals, despite of depicting some challenges in generalizing the data collected from exercising the method.

3.7.1.4 Purpose of the Focus Group

The purpose of the focus group session was to interact and discuss on the current state of privacy, security, and data protection in the software as a service security as required by emerging regulations, standards and frameworks. The results of this focus group session are intended for requirements gathering towards designing a novel security and privacy compliance tool for software as a service business applications. The focus group session aimed to provide additional data collection support to the data collected from the questionnaire.

The focus group had participants who constituted senior IT managers and decision-makers from highly strategic organisations in Nigeria to obtain specialist and professional inputs into the design and implementation of the proposed privacy and security compliance mechanism. See **Table 5** below for descriptions of participants’ organisations.

3.7.2 Data Analysis Methods

3.7.1 Questionnaire Analysis

Questionnaire analysis was conducted using Microsoft Forms, which has a data analysis feature at the backend that streams data directly. This provided the researcher with rich, high-end visualisations in the form of charts (Jennifer Rowley 2014).

3.7.2 Focus Group Analysis

The researcher transcribed and generated data from the focus group session's audio recording and formatted them by referring to the UK Data Archive’s guidelines and suggestions on transcription conventions (UK Data Archive 2007). The researcher transcribed the audio data and imported them into a computer-assisted qualitative data analysis software (CAQDAS), NVivo, to analyse them and find recurring themes and patterns.

The data were coded, organised, and labelled for interpretation. In NVivo, extracting, labelling, and classifying as coding are the most critical steps in analysing qualitative data. These steps allow the researcher to organise the transcribed data's text and discover patterns that may not be visible or detectable by just reading the text or listening to the audio.

The researcher relied on NVivo to categorise the focus group data. Additionally, NVivo helped identify meaningful patterns from the data (Jarzebowicz, 2017). The researcher used the focus group session where the questionnaire data were not sufficient (Krupp, et al. 2017).

3.7.3 Participant Organisations

Table 6: Participant organisations

S/N	Organisations	Who They Are/What They Do	Significance of Response
1	**Nigerian National Petroleum Corporation (NNPC)**	NNPC is the state oil corporation.	High
2	**Nigerian National Petroleum Corporation – RETAIL (NNPC Retail Ltd.)**	NNPC Retail Ltd., is a fully owned subsidiary of NNPC.	High
3	**National Information Technology Development Agency (NITDA)**	NITDA was created in April 2001 to implement the Nigerian Information Technology Policy and co-ordinate general IT development in the country.	High
4	**Nigeria Content Development Management Board (NCDMB)**	NCDMB was established by the Nigerian Oil and Gas Industry Content Development Act, which came into effect on 22 April 2010.	High

3.7.4 Evaluation

The artefact was evaluated using two evaluation tools: a case study and semi-formal proofs. The evaluation's objective was to determine whether the artefact and design process advanced in this study were fit for specifying and matching the privacy and data protection compliance properties of the service provider and the preferences of users within the context of the NDPR and SaaS applications.

3.7.5 Case Study

To show the utility and provide a context for the artefact and semi-Semi-formal concepts designed based on the regulatory requirements of the NDPR and therefore, the NDPR requirements were expressed and using SaaS-PPL. The case study assume a scenario where a customer interacts with a SaaS-enabled pay-at-the-pump POS solution to pay for services at a petrol station.

3.7.6. Semi-Formal Proofs

Semi-formal proofs (Hales 2008b) techniques helped the researcher match SaaS service providers' privacy policy preferences with data subjects' preferences by matching the SaaS service provider policy. It was less (or equally) permissive as the data subject's security and privacy preferences as captured in the NDPR.

3.7.7 Planning for the Focus Group Session

The focus group session's objective was to get participants to interact and discuss current security and privacy concerns in SaaS applications offered by leading service providers. The results were intended to meet the requirements for designing a compliance mechanism for SaaS business applications.

The focus group session took place in Abuja, the Federal Capital Territory, Nigeria. The participants were drawn from both the private and public sector of the industry, including relevant regulatory agencies.

3.8 Chapter Summary and Conclusion

In this chapter, design science and semi-formal methods were introduced as the current research study's preferred methods. The research focuses on designing a policy language for the specification of compliance properties, referred to as the 'artefact'. The design science and semi-formal methods were applied to the NDPR data protection requirements using a petrol station scenario. The following chapter will provide the results of the data collected at the data-gathering stage.

CHAPTER FOUR

4.0 SaaS-PPL Requirements

4.1 Introduction

In this chapter, the privacy and data protection principles of the NDPR are discussed in detail. Additionally, the rights of data subjects whose personal data are collected are discussed alongside the obligations of the service provider in the NDPR. The transfer of personal data to third parties or countries, an essential cornerstone of privacy and data protection, is also discussed in detail. Finally, the chapter introduces the concept of the data life cycle and all the stages involved therein. The researcher relies on the data life cycle concept to map and align the stages of data life cycle NDPR requirements of the specification policy language.

4.1.1 Lawful Principles of the NDPR

Like other data protection regulations, the NDPR introduced legal data processing principles, particularly personal data processing. It also introduced other principles such as consent collection from data subjects, legitimate purposes for data processing, transparency and the minimisation of data collection, and the duty of care and accountability to any person or entity entrusted with personal data.

4.1.1.1 Scope of the NDPR

The scope of the NDPR applies to any organisation handling the personal data of Nigerians. Meanwhile (Nigerian Information Technology Development Agency 2019), the GDPR has a global impact and applies to organisations even outside the EU that handle the personal data of EU citizens. Furthermore, sections 1.1, 1.2, 1.3, and 4.1 of the NDPR and Articles 3 and 4 (1) of the GDPR clearly state that the regulations only protect and safeguard individuals’ rights, not those of legal persons or entities. Whereas the NDPR does not distinguish between private and public bodies, the GDPR applies majorly to public bodies. Therefore, in terms of scope, the two regulations are reasonably consistent.

4.1.1.2.1 Regulatory Scope

Although the two regulations' scopes apply to organisations that personal process data, usually referred to as data controllers, the NDPR applies only to organisations and citizens within the Nigerian state's jurisdiction. In contrast, the GDPR applies to all people referred to as natural persons in the regulations' text irrespective of their nationality.

4.1.1.2.2 Jurisdictional and Territorial Scope

All NDPR provisions and principles apply to the processing of personal data of living persons in Nigeria, as outlined in Section 1.2 of the regulation, and the processing of Nigerians living outside of Nigeria. Meanwhile, the GDPR (Articles 3, 4, & 11 and Recitals 2, 14, & 22–25) extends outside of the territorial boundaries of the EU and is thus applicable to data controllers without operations in the EU

4.1.1.2.3 Material Scope

The NDPR and GDPR define 'processing', sensitive personal data, and personal data in the same way. However, in the NDPR, there is no emphasis on the processing of data by other means, such as non-automated means.

4.1.1.2 Evaluation of the NDPR and GDPR Data Protection Principles

From the legal perspective, data protection regulations are meant for legal experts and are subject to legal and ambiguous interpretations. These interpretations further compound the challenges facing their compliance. For example, the NDPR and GDPR aim to protect personal data by requiring compliance from organisations involved in collecting, using, storing, and forwarding personal data. They apply to contexts where personal data are either collected online using electronic means or collected offline. Whereas the NDPR came into effect in April 2019, the GDPR came into effect in May 2018. Both regulations share very similar objectives. The NDPR's sole objective is to safeguard the privacy of data relating to natural people in Nigeria. It seeks to achieve this by ensuring that all transactions involving personal data transfer are free from manipulation. The regulation also stipulates a penalty for violation: 2% of annual gross revenue for data controllers who handle personal data of at least 10,000 users of a service and 1% of annual gross revenue for data controllers handling fewer than 10,000 users.

The GDPR primarily aims to protect residents' privacy within the geographical space of the EU by regulating how organisations handle and process personal data in their operations. The EU is a significant economic bloc; therefore, the GDPR's reach and impact are global. As highlighted above, the two regulations are similar in many areas, such as their objectives, definitions of terminologies, scopes, and safeguards to protect natural persons' right to data privacy. However, they are different in many areas as well, such as in enforcement mechanisms and authorities, child rights, and penalties for violations. In the following sections, these similarities and differences are discussed.

4.1.2 Key Definitions of Terms in the NDPR and GDPR

Both the NDPR and GDPR have similar definitions, with two key differences: the definition of a child and a data processor's definition. Whereas a data processor's role is the same as that of a data controller in the NDPR, the GDPR classifies them separately.

- **Personal Data:** In Section 1.3, the NDPR refers to personal data as any form of data that can be directly or indirectly associated with a living person, such as full names, national ID numbers, phone numbers, IP addresses, and email addresses (Skendžić, et al.

2018, L. Elluri, Nagar et al. 2018b, NITDA 2019). Additionally, in the NDPR, no information on data is ‘anonymised’, whereas in Article 4 and Recitals 26–30 of the GDPR, anonymised data are defined as data that cannot identify a person, such as sensitive records (e.g. past criminal records).

- **Data Subject:** This refers to a person who can be identified by any information obtained from social, economic, physical and cultural, or electronic devices (e.g. IP addresses) (Jayasinghe, Lee et al. 2018).
- **Data Controller:** A data controller is a person or entity that handles personal data relevant to their operations.
- **Data Processor:** The NDPR does not distinguish between the data processor’s roles and the data controller’s roles. Section 5 includes all entities that process data as data processors or controllers. In comparison, a data processor role is described in the GDPR as a legal person (Altorbaq, et al. 2017c).
- **Child Definition:** The NDPR does not specially recognise children as natural persons requiring superior data protection. It merely contains provisions for all-natural persons. Meanwhile, the GDPR recognises children as natural persons who are vulnerable and require superior data protection. This special protection should have applicability to marketing or services tailored for children (Papadimitriou,et al. 2019).

4.1.2.1 Data Subjects’ Rights in the NDPR

In the NDPR, data subjects have been given rights such as the right to access information relating to processing and to be informed where no action has been carried out on a request to a data controller. Other rights are the right to withdraw consent, the right to rectification of processing, the right to deletion or erasure, the right to know what the interests of a data controller or entity are, and, finally, the right to restrict or even object to any form of processing.

4.1.2.2 Enforcement in the NDPR

Enforcement is the actual process of ensuring compliance with regulations. The NDPR and GDPR both contain monetary penalties for non-compliance, but the penalties, procedures, and amounts differ significantly.

- **Monetary Penalties:** The NDPR imposes a flat rate of 10 million naira or 2% of the annual revenue of the previous year (Nigerian Information Technology Development Agency 2019). Similarly, the GDPR imposes a flat rate of 10 million euros or 2% of the annual revenue of the previous year (or 20 million euros or 4% of annual turnover, whichever is higher) in the case of a company with global operations.
- **Supervisory Authority:** The NDPR does not have any provisions for establishing an independent monitoring authority, but it does mandate the NITDA to oversee the application of the NDPR. In contrast, Article 51 provides for an independent authority to implement the GDPR in the EU. The authority is responsible for assisting organisations in understanding their obligations and compliance.

4.1.2.3 Civil Remedies in the NDPR

To persuade or coerce relevant parties to take responsibility, provisions for civil remedies are included in the NDPR as well as the GDPR. They allow individuals to seek redress for violations of their privacy or the privacy of their data. According to Section 4.2 of the NDPR, the right to seek redress is affirmed, while NITDA retains powers to set up an investigative administrative redress panel to investigate violations (Nigerian Information Technology Development Agency 2019). Similarly, Articles 79–82 and Recitals 141–147 (Kovačić et al. 2018) of the GDPR state that a violation is a justifiable cause to start legal action.

4.1.2.4 Data Controllers and Processors in the NDPR

The NDPR and GDPR share some similarities regarding the scopes and responsibilities of data controllers.

The scopes of the NDPR and GDPR are common when it comes to data controllers. Additionally, both the NDPR and Data protection officer (DPO) mandate the use of a data protection officer. The NDPR does not use the term 'data processor', but rather 'data administrator'. The GDPR also introduces the concept of data protection impact assessments, which is missing in the NDPR. However, the NDPR mandates that controllers perform a complete privacy and data protection audit within six months of the implementation date of the NDPR.

The NDPR has significant implications for controllers and processors when it comes to their responsibilities. Additionally, they must believe that data protection should be enabled by default, which implies that all technologies should be equipped with security measures at the time of their design. A controller should process-specific data for a specific purpose only, and the subject must be informed in the event of a data breach.

4.1.2.5 Transfer of Personal Data in the NDPR

According to the NDPR and GDPR, personal data may be transferred to third countries (Sections 2.11, 2.12, and 4.3 of the NDPR and Article 44–50, Recitals 101 and 112 GDPR). Transfer of personal data must be made to a third country or jurisdiction that meets the relevant authority's standards of protection. However, under the NDPR, grounds for a cross-border transfer do not include a transfer being made from a register accessible by the public or by a person who can demonstrate a legitimate interest.

Inside the EU, the GDPR has made the process of transferring personal data complex. It is only allowed when certain conditions are met, for example, evidence of adequate safeguards, adequacy decisions, treaties, and unique situations or circumstances.

An adequacy decision situation is when the European Commission decides that a country has satisfied the adequacy conditions. In this situation, personal data transfer may be allowed if evidence of enforceable rights has been made accessible for data subjects. If none of the above applies, under the NDPR and GDPR, eventual transfer of data may happen, but only on the judgement or order of a relevant court of law.

4.1.3 Data Life Cycle

Data life cycles are the sequences that a unit of personal data goes through, from when it was initially collected to how and where it was stored and used (B. Spasic, et al. 2018b). According to Butin *et al.* (2015), personal data protection can only be beneficial when organisations implement protection policies at each stage that makes up the life cycle of personal data.

Furthermore, regarding how organisations share data with third parties and how they are deleted or erased, Butin (2015) argue that regulations help set obligations. These obligations can help in the exercise of responsibility and the verification of handling practices by organisations regarding personal data.

In this study, the proposed policy language specifies policies on the stages of the data life cycle (e.g. data collection), policies enforcing storage preferences (e.g. preferred location), policies for enforcing usage of collected data, and policies for deletion and forwarding of data to third parties.

4.1.3.1 Data Collection

Section 2.3 of the NDPR requires data controllers to clarify their purpose before collecting personal data; it also requires them to clarify how they intend to process the data. Furthermore, to avoid random and excessive data collection, the regulation seeks to limit data collection to the purpose of collecting (NITDA, 2019).

4.1.3.2 Data Usage

In Section 2.1 (subsection (a)) of the NDPR, data controllers are requested to collect data according to a clear lawful purpose. This purpose is to be communicated and have the consent of the data subject. A service provider’s policy should have indicated details on (i) consent for use, (ii) purpose, and (iii) who will use the data (Salami, 2020).

4.1.3.3 Data Storage

In Part 2, Section (12), the NDPR declares that personal data should be stored only for the amount of time reasonably needed to store them. In a situation where a specific type of data is stored by a data controller or SaaS service provider, (i) the location of storage must be known, (ii) the storage infrastructure must be secure, and (iii) a periodic review must be conducted of the reasons the personal data are in storage (Agbali, Dahiru et al. 2020). Furthermore, the NDPR states that where processing has been restricted, such personal data shall, except for data stored, only be processed with the data subject’s consent.

4.1.3.4 Data Deletion

Section 3.1 (9) of the NDPR also describes the rights that data subjects can exercise regarding the erasure or deletion of their data from a service provider's infrastructure (Izuogu, 2021). Therefore, by implication, service providers are required to have mechanisms or provisions for the enforcement of these rights based on (i) who is authorised to delete data from a service provider’s storage system, (ii) what type of data is authorised personnel allowed to delete or retain, and (iii) whether the deletion is subject to a period of delay(NITDA, 2019).

4.1.3.5 Data Forwarding

Services and service providers continue to depend on each other to benefit users, making the need to share data among service providers critical (Breaux, 2016). To ensure effective regulation and protect data subjects' rights, data protection regulations require that consent be obtained for data forwarding. In Sections 2.11 and 2.12 of the NDPR, data forwarding criteria describe the conditions in which a service provider or a data controller may transfer personal data to a third-party recipient. Some of the conditions are (i) consent provided by the data subject, (ii) a specific purpose stating why the data will be forwarded, and (iii) a list detailing the recipients of the personal data (NDPR, 2019).

4.1.4 Mapping of Legal Compliance Properties of the NDPR

SaaS application service providers collect and process users' data to provide their applications or services, thus creating the need for ensuring compliance with data handling regulations. This research focuses on a scenario where data are collected and transferred from the data subject to the service provider's infrastructure. The transfer method can conflict with the data handling preferences of the data subject, thus raising security and privacy concerns (Daibouni, et al. 2016).

Following the analysis of the obligations of data controllers set out in the NDPR (see sections 5.1.3.1 to 5.1.3.5), the proposed policy specification language, SaaS-PPL (Tøndel et al. 2017), will be used to express rules that correspond to the collection, usage, storage, deletion and retention, and forwarding of data.

Further analysis of the data protection and handling expectations of the NDPR showed that the NDPR requires the proposed policy language to express data compliance rules relating to the collection, usage, retention, and storage location. PPL (Benghabrit, et al. 2014) meets some of these requirements, for example, access control and authorisations. Moreover, the policy language should be extensible enough to meet the NDPR's requirements regarding SaaS applications. The requirements are by no means exhaustive, but they satisfy the contextual objective of checking for compliance with data protection regulations in SaaS applications.

4.1.4.1 Requirement #1: Data Collection

Organisations are facing challenges relating to consent and opt-out rights (Altorbaq, et al. 2017b). A critical issue relating to data collection is obtaining consent when processing personal data. According to Section 2.3 of the NDPR, the data subject's freely and unambiguously given consent in writing, by e-mail, or orally is required to process their data (Skendžić, et al. 2018, NDPR, 2019). The consent may be withdrawn at any given time (see Part 3, Section (i) of the NDPR), which creates a compliance challenge in cases where third-party processing has already taken place. The SaaS-PPL specification language has a sub-policy for obtaining consent to fulfil the compliance requirement of the NDPR.

4.1.4.2 Requirement #2: Data Processing

To use SaaS applications, organisations collect and share data with service providers. This poses the challenge of conflicting interests relating to usage and processing and raises concerns about how the service provider and other third parties may use the collected personal data. According to Part 2, Section 2.2 (subsections (a–e)) of the NDPR, the service provider must have a lawful basis and obtain consent from the data subject before processing personal data. The proposed SaaS-PPL extension will have sub-policies and elements to specify (i) who can process personal data and (ii) what the purpose of the processing is.

4.1.4.3 Requirement #3: Data Storage

According to Part 2, Section 7 (subsection (h) and Section 12 of the NDPR, organisations must enforce data protection when they collect, store, or process data, and they may only collect data for certain such as storage purposes. In SaaS applications, SaaS service providers' regular make data copies and backups usually contain personal and usage data to achieve service availability (Sultan A 2016). While data availability and integrity are the aims of continuous backup, they come with compliance and consent collection challenges, especially when third-party storage services are involved (Li, et al. 2015). The proposed SaaS-PPL will have policies detailing where a particular data type is stored, how it is stored, and how long it is stored. Periodic reviews of the policies will be conducted.

4.1.4.4 Requirement #4: Data Retention and Deletion

Part 2, Section 7 (subsection (h) of the NDPR deals with the data subject's right to be forgotten, to erasure, and to retention or deletion (NDPR, 2019). (Sarkar, et al. 2018) claims that the data subject has the right to request the controller to erase any personal data the controller may possess without undue delay. The proposed SaaS-PPL will have a sub-policy for specifying who can delete data, how the data are to be deleted, what the delay period for retention is, and the worst-case deletion scenario is.

4.1.4.5 Requirement #5: Data Forwarding

In the last stage of the data life cycle, data forwarding or transfer happens when a service provider transfers or shares data with a third party for processing (DLA Piper, 2020, Di Iorio, Carinci et al. 2020) . Part 2, Section 7 (subsection (e)) of the NDPR sets out the requirements for data forwarding or transfer by a service provider to a third party. It states that any transfer of personal data that are undergoing processing or that are intended for processing after transfer to a third country or an international organisation shall take place subject only to the rights of the data subject, such as the right to know the legitimate interests of the third party, the right to know the recipients or the category of the recipients, and the right to know about the existence or absence of an adequate decision on international transfer of data by NITDA when the transfer is to a third country or international organisation (Asuquo 2019).

SaaS-PPL is obligated to provide the list of recipients, specify the transfer or forwarding purpose, and provide the corresponding records of the data forwarding process.

4.2 Chapter Summary

In this chapter, the NDPR (2019) principles were presented and evaluated against the GDPR principles. The NDPR’s scope, including personal, material, and territorial scope, and its applicability were discussed. Furthermore, definitions of key terms of the NDPR, such as rights, enforcement mechanisms, civil remedies, data subjects, data controllers, and processors, were mentioned, and the issue of how third-party data transfers can be executed was explored. Other concepts, such as the data life cycle and the mapping of compliance requirements and properties based on the legal basis provided in the NDPR, were also presented.

CHAPTER FIVE

5.1 Data Collection Analysis and Results

5.1.1 Introduction

This chapter presents findings from the research. The findings can be divided into two groups based on the data collection instruments, qualitative and focus group session. Figure 14 illustrates how these two types of results are integrated. According to this figure, the results, from the questionnaire were supported with the results from the focus group to arrive at the specific set of requirements for the design of the SaaS-PPL. Additionally, there are many overlapping findings and themes between each data collection method, therefore, the findings are divided into two groups: 1) findings from the questionnaire, 2) findings from the focus group session. The results are then analysed and discussed.

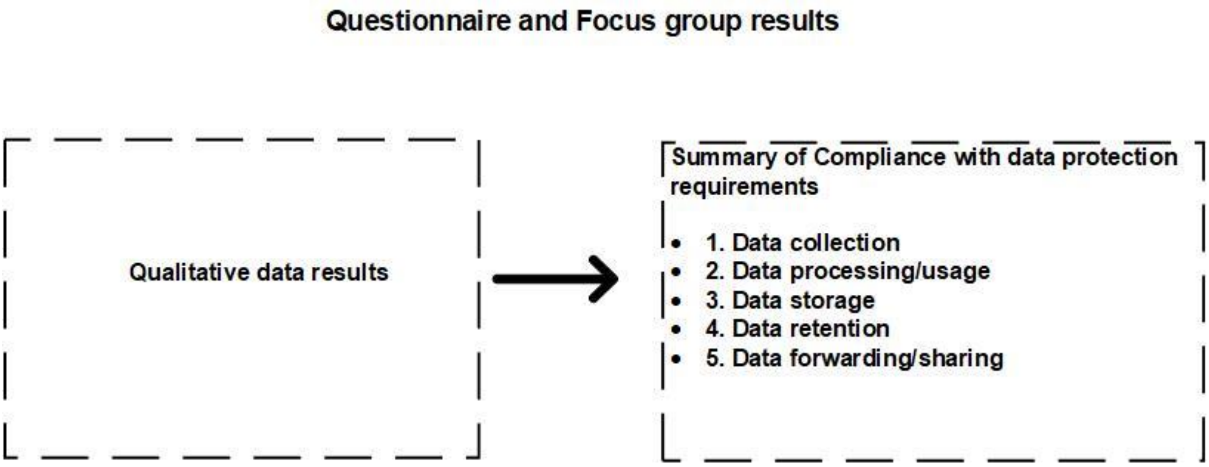

Questionnaire and Focus group results
Qualitative data results
Summary of Compliance with data protection requirements
• 1. Data collection
• 2. Data processing/usage
• 3. Data storage
• 4. Data retention
• 5. Data forwarding/sharing

Figure 14: Integration of Qualitative Data results

5.1.2 Data Collection tools

For the purpose of achieving the objectives of this research the researcher collected data using two qualitative instruments, the questionnaire and the focus group. In the questionnaire are questions were asked from a number of sections such as on SaaS applications, SaaS privacy and security issues, existing privacy and security compliance efforts of organisations and service providers with relevant data protection regulations (See Appendix 4).

On the other hand, the focus group was used to ask additional questions relating to existing security compliance standards, frameworks, and data governance issues for SaaS applications relevant to the retail sector and to what extent are these issues inhibiting the adaptation of SaaS applications in the Industry (See Appendix 5)

5.1.3 Questionnaire Instrument

A structured set of questions was used to gather the relevant data for this study. This was used to direct the respondents to provide relevant data that will be analysed in the study for the purpose of extracting concerns and requirements towards a solution to compliance with data protection regulations. This saves time and effort as well as preventing bias while asking questions through personal interviews.

Furthermore, from the literature review and other relevant materials , questions were developed in order to evaluate the constructs of this study. These include SaaS applications, issues such as privacy, security, and compliance with data protection regulations. Other areas include standards, frameworks, and regulations and their impact on SaaS adoption in a retail context.

5.1.3.1 Questionnaire Structure

The questionnaire was divided into 4 sections with each section separated by a specific heading. In Section 1 consisted of 10 questions used to assess the stage of adoption of SaaS and generally cloud computing in the organisation. Respondents were required to select from a list of option radios to indicate the stage of adoption in the organisation. Other questions in the section require repondents to rate the different service models according to the order of preference and use within their organisation. Ranking them from 1 to 5, with 1 being most important and 5 being the least important.

Furthermore, In Section 2, 28 questions were asked on issues such as privacy, security, availability, were asked. Additional relevant questions were raised on specific solutions to privacy and security, and how authentication is implemented when accessing SaaS applications. In Section 3, 7 questions were asked on compliance and on how compliance with data protection regulations is achieved. Additionally, within the section, questions on evidence of verification of compliance by the service provider were included.

In Section 4, respondents were asked questions relating to specific controls, standards and framework to gather information on how the models. Options on frameworks, standards and controls were provided for respondents to select.

5.1.3.2 Scaling of Measurement

All statements and questions in sections 1, 2 and 3 were developed using a five point Likert scale. For the purpose of data interpretation, the descriptive phrases for the main side of the five-point scale are (1) “most important”, (2) “slightly important”, (3) “very important”, (4) “important”, and (5) “least important”.

In Section 4 , questions asked relating to controls, standards and frameworks developed using 5 options such as a simple “Yes , “No”, “Not sure”, “Others”, “Please specify”. Others are simply 5 options of solutions of technologies that apply to the questions such as “LDAP”, “On-Premise AD”, “Azure Cloud AD”, “Single-Sign-On”or “’Not Sure” where the respondent is not sure.

5.1.3.3 Pre-Testing the Questionnaire

Prior to activating and disseminating the questionnaire, pre-testing was undertaken with the supervisory team and the University of Central Lancashire's ethical committee. Pre-testing is used to get feedback on the questionnaire's comprehension, wording, and design. In other words, the pre-test was designed to:

i. Examining the questionnaire's content validity
ii. Verification of completeness, syntax mistakes, and overall layout format.
iii. Assuring that the questions are comprehended and interpreted appropriately

5.1.3.4 Data Screening and Checking

Data were screened and checked to ensure they were free of mistakes, since inaccuracies might arise during data input, jeopardising the analysis.

5.1.3.5 Questionnaire Data Analysis

Data analysis is a carefully planned step in the research process (Pat and Jackson, 2013). The data analysis process was motivated by the study's objective of providing pertinent information to address the issue. The purpose of any analytical method is to convert data information needed to make decisions

The Questionnaire was downloaded from Microsoft Forms platform and imported in NVivo alongside the transcript from the audio record of the focus group session. This is in addition to the questionnaire analysis automatically carried out by Microsoft Forms, which has a data analysis feature at the backend that streams data directly. This provided the researcher with rich, high-end visualisations in the form of charts (Jennifer Rowley 2014).

5.1.4 Focus Group Protocol

The purpose of this focus group session is to interact and discuss on the current state of privacy and privacy in SaaS application’s privacy and security capabilities offered by leading SaaS service providers in the retail sector. The results of the focus group session are intended for requirements gathering towards designing a novel privacy and security compliance tool for SaaS business applications.

5.1.6.1 Phase 1: Identification and Selection of participants

Participants were invited as part of a sample size, who work with an oil company, or an oil and gas agency in Nigeria, particularly the retail sector of the industry. Additionally, they were selected based on their roles in operations, IT, and management level staff of their organisation.

S/N	Organisations	Who They Are/What They Do	Significance of Response
1	**Nigerian National Petroleum Corporation (NNPC)**	NNPC is the state oil corporation.	High
2	**Nigerian National Petroleum Corporation – RETAIL (NNPC Retail Ltd.)**	NNPC Retail Ltd., is a fully owned subsidiary of NNPC.	High
3	**National Information Technology Development Agency (NITDA)**	NITDA was created in April 2001 to implement the Nigerian Information Technology Policy and co-ordinate general IT development in the country.	High
4	**Nigeria Content Development Management Board (NCDMB)**	NCDMB was established by the Nigerian Oil and Gas Industry Content Development Act, which came into effect on 22 April 2010.	High

Generation of questions

Questions were generated based on the purpose and goals of the focus group session**.** Consent forms (See Appendix 8) were also provided to collect their consent to take part in the focus group session. However, as participation is voluntary, participants were informed of their right to withdrawal from the session.

5.1.6.2 Phase 2 : Conduct of the Focus group Session

The researcher served as the for discussion alongside an assistant moderator who was engaged to handle logistics and to take notes. The assistant was also responsible for setting up the venue and with assisting participants to settle in the venue (See Appendix 6). The entire duration of the session lasted approximately to 1 hour, and themes and questions will focus on Software as a Service, Security and Privacy Compliance and issues bothering on ensuring compliance by service providers.

5.1.6.3 Phase 3: Analysis and reporting Focus group results

The data collected from the focus group session were transcribed and generated from the audio recording of the focus group session and formatted in line with the UK Data Archive’s guidelines and suggestions on transcription conventions (Corti, et al. 2019), (UK Data Archive 2007). The transcribed data were then imported into a CAQDAS, NVivo, to analyse them (A. Jarzebowicz, K. Polocka 2017). The researcher used the focus group session to supplement and triangulate the data where the questionnaire data were insufficient (Krupp, Rueben et al. 2017).

Thematic analysis was conducted in line with (Maguire, 2017) and followed the methodology section discussed in Chapter 3. The findings that emerged from the questionnaires and focus group were used to meet the requirements for designing a compliance specification language for SaaS business applications in the early stages of the research. This effort eventually led to the research focus on the NDPR (2019) and data protection legal compliance requirements.

The data is presented and triangulated with data from the focus group session in the sections below.

5.1.4.1 Example of Questionnaire questions

***Q17. Is there an evidence from your SaaS service provider that all network transfer of your Data is private and encrypted when traversing the Service provider's network?**

Yes □

None □

Not Sure □

Others □

Please explain briefly

***Q18. Does your SaaS service provider implement appropriate controls to ensure data integrity (e.g. input validation, transaction redo logs)?**

Yes □

No □

Do Not Know □

Other (Please specify) □

Please explain briefly

5.1.4.2 Example of Focus group questions

Introductory questions	Questions
	1. What is your most important concern in the Oil and Gas Industry when it comes to adopting Software-as-a-service application in your retail operations? 2. How concerned are you within this industry regarding privacy and security in the cloud, particularly in Software-as-a-service business applications? 3. How is your concern for security impacting your decision to adopt Software-as-a-service into your operations? 4. In what areas of your retailing operations do you use Software-as-a-service?
Main Questions	1. How concerned are you about the location of your operational data? 2. What technical enforcement mechanisms does your cloud service provider use to prevent access to your data by other users residing on the same hardware due to multi-tenancy? 3. What established frameworks does your cloud service provider use for the enforcement of security and privacy controls? 4. How do you ensure compliance with those data protection regulations, frameworks and standards? 5. Does your cloud service provider ensure compliance with third-party audits or an automated tool?
Closing Questions	1. Can you as a customer audit the Cloud Service Provider’s in-house security controls? 2. Can automation of some specific controls from standard security frameworks help improve the security of your data? 3. Will you move all your business applications into the cloud if you can verify compliance using an automated tool? 4. Are there other concerns apart from security and privacy issues that are hindering your migration to the cloud and using software-as-a-service?

5.1.5 Participants and Sample Selection

The data collection and research focus was on the retail sector within Nigeria. It would be impractical to invite every participant organisation in the sector due to limitations of potential reluctance of organisations to participate, time, resources and some Nigeria specific socio-political challenges at the time of the conduct of the research.

The method of purposive sampling was used to identify and develop the sample of respondents and focus group participants for the research. Purposive sampling methods is a kind of non-probability sampling in which researchers choose individuals or organisations of the public to participate in surveys of focus group session based on their own assessment (Campbell, Greenwood et al. 2020)

Participants were drawn from people who work with an oil company, an IT agency or company in Nigeria, particularly the retail sector. Additionally, participants were selected based on their roles in the areas of operations, IT, and management level of their organisation. All participant data was collected between August 2018.

5.1.6 Ethical Approval

Further, the research was subject to ethical considerations regulations of the University of Central Lancashire and relevant data protection regulations such as the NDPR and the GDPR which led to the approval of the study by the University Ethics committee (See Appendix 2).

As indicated in Chapter 3, a consent page was provided to each client before the completion of the questionnaire and personal information sheets were provided to focus group participants detailing the objectives and purpose of the research, and to reassure the participants that their participation is voluntary and that they can withdraw any point in time during the focus group session. Additionally, participants were also informed that their answers will be treated as confidential and treated with anonymity and only for the academic purpose for which it was obtained.

Finally, participants were not harmed, both physically and psychologically during the entirety of the conduct of the research.

5.2 Discussion of Results

As stated in Chapter 1, the overall aim of this thesis is to design an extended, semi-formal policy language approach to privacy and data protection compliance for SaaS business applications by expressing requirements for a) the privacy of personal data and b) the achievement of compliance with data protection regulations that relate to the privacy of personal data and in other to achieve the above aim, the research set out to answer the following questions.

First, to identify the legal and textual requirements of the NDPR, as they relate to the principles of Privacy by Design. Second, to find out how the legal requirements of the NDPR can be mapped and aligned to the data life cycle. Third, find out how privacy and data protection requirements can be presented in a semi-formal policy language. Finally, how to model of the compliance check syntax show proof of compliance when all properties are matched and validated within the context of SaaS applications. Based upon these, the findings of the study are discussed as follows:

5.2.1 Compliance Requirements

Compliance typically involves complying or adhering to industry standards and regulations or laws (Jansen, Grance 2011). In the context of SaaS applications, existing approaches such as SLAs are used to guarantee the rights of users and the obligations of service providers (Heyink 2012). SLAs are therefore used to measure service levels provided by the service provider. Other issues such as availability, response time, QoS, downtime, security, and data location are a part of the SLA (Trapero, et al. 2017). However, the challenges of verifying security and privacy compliance remain a significant impediment to SaaS applications and their adoption (Yimam, Fernandez 2016). It is against this backdrop that governments and industries have enforced several laws and regulations regarding administering and compliance with data security and privacy, especially in SaaS applications.

5.2.1.1 Questionnaire Data

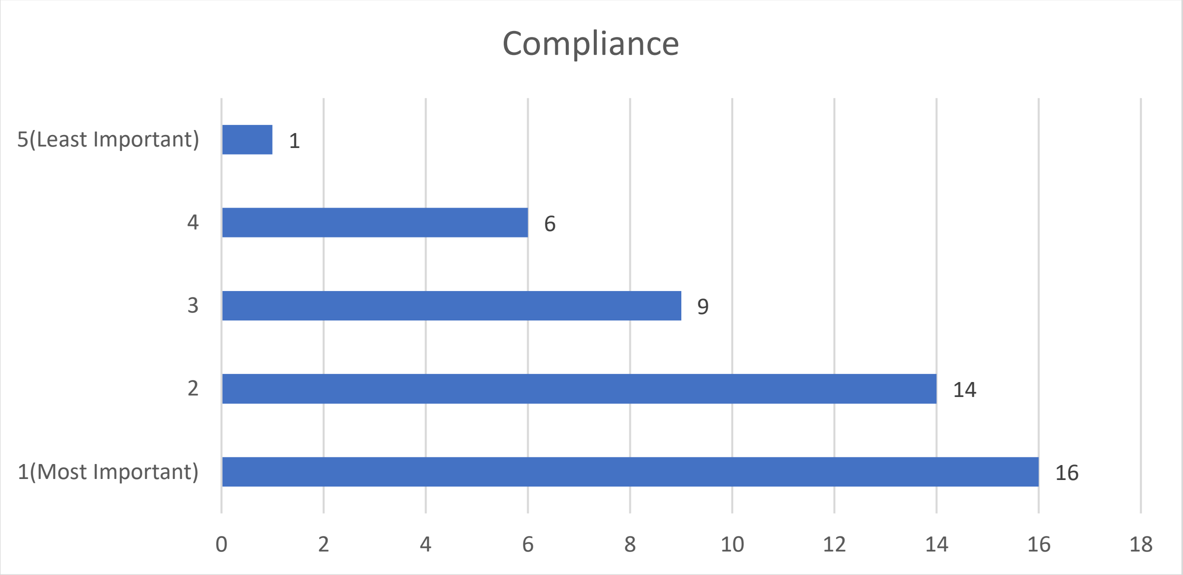


Figure 15: Compliance barrier

According to Figure 15, 65% of the respondents considered compliance a significant barrier. A further breakdown shows that 34.8% considered it the most critical barrier, and 30.4% considered it a significant barrier. A total of 19.6% neither agreed nor disagreed that compliance was a significant barrier, whereas 13% said it was somewhat unimportant, and 2.2% said it was less critical to their decision to adopt SaaS.

5.2.2.2 Focus group data

A compliance theme emerged in the analysis of the transcript data of the focus group. Participants discussed compliance tools, regulations, and frameworks and how they ensure compliance in their organisations.

They explained that, currently, they mostly used SLAs to ensure compliance.

They confirmed that they did not currently use any tool to verify compliance with SLA provisions. One of the participants said they aligned their infrastructure and operations to work with Information Technology Infrastructure Library (ITIL) and Projects in Controlled Environment 2 (PRINCE2) and that they were considering relevant frameworks designed for the cloud, such as the Cloud control matrix (CCM). This alignment was in preparation for the eventual adoption of SaaS applications across the participant's operations. Participants expressed a unanimous desire for an automated means of verifying compliance with the SLA provisions they signed with providers and data protection regulations.

5.3 Security Barrier

5.3.1.1 Questionnaire Data

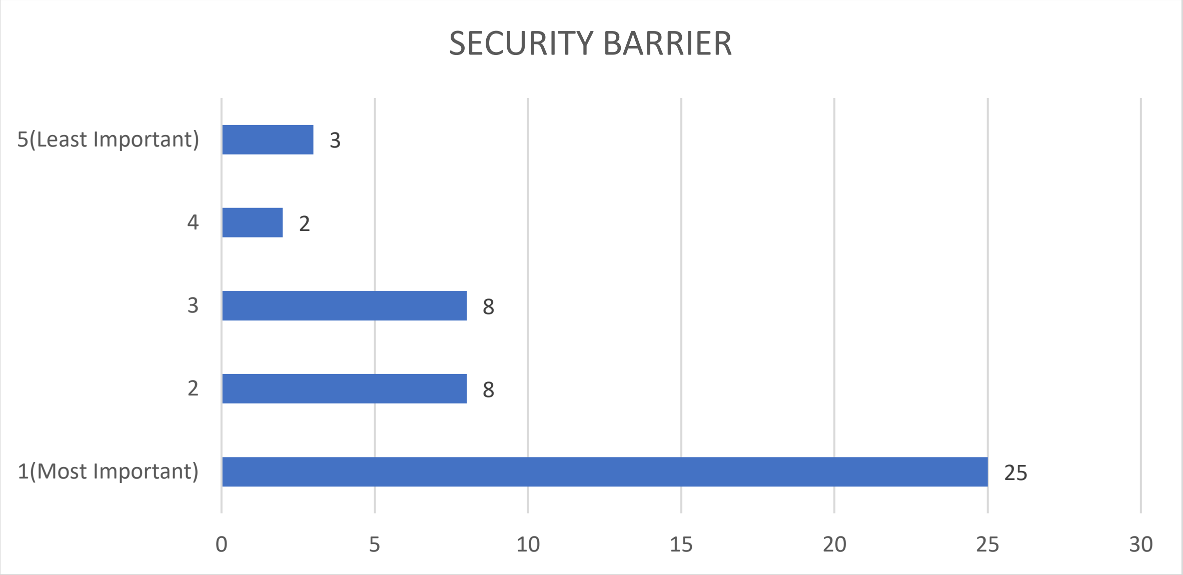


Figure 16: Security barrier

As shown in Figure 16, respondents were asked to rank the five most important factors or barriers to SaaS adoption, with one being the most important and five being the least important.

A total of 71.9% of the respondents said security is the most critical barrier to adopting SaaS applications in their organisations compared to the reliability, interoperability, performance, and so on. A total of 17% considered security to be necessary, and 54.9% considered it to be most important. A total of 17% neither agreed nor disagreed that security was a barrier to adopting SaaS, 4.3% said it was somewhat unimportant, and 6.8% said it was least important.

5.3.2 Focus Group Data

Participants indicated they were hopeful that SaaS applications' security would improve because this would significantly affect their decision-making process regarding SaaS adoption. Participants also indicated that they were planning broad adoption and integrating SaaS into their operations. They also seemed optimistic that if appropriate specific controls were automated, especially those pertaining to existing regulations, it would help drive their adoption and reduce security concerns.

5.4 Privacy Barrier

5.4.1 Questionnaire Data

As shown in Figure 15 below, respondents were asked to comment on whether their service provider offered any evidence of their data encryption when they were traversing the service provider’s network. A total of 48% said the transfer of their data was encrypted when traversing the service provider’s network, 22% said their data were not encrypted, and 30% said they were not sure.

Therefore, a total of 52% indicated that they lacked evidence to prove that their service provider was keeping their data private and or their data is encrypted. This added to their privacy concerns concerning SaaS applications, as indicated in Figure 17 below.

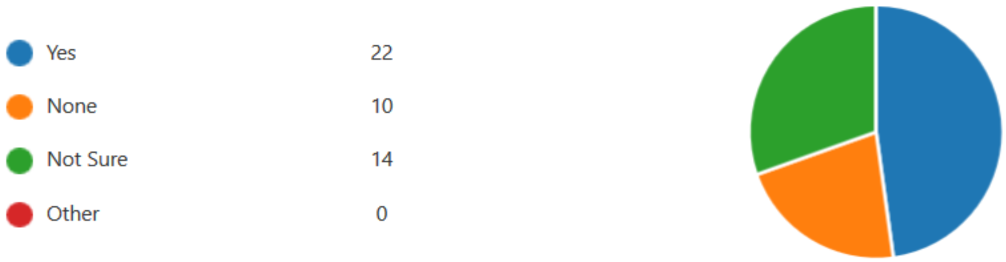


Figure 17: Privacy barrier

5.4.2 Focus Group Data

Respondents agreed that privacy was a major issue in SaaS applications, including the need to protect personal data and transaction histories. Many organisations are not comfortable storing their data and applications on systems that reside outside their infrastructure and control (Takabi, Joshi et al. 2010).

During the focus group session, respondents indicated they were bothered about the privacy of their data. The analysis of the focus group data revealed a theme related to privacy concerns. Other concerns respondents revealed pertained to infrastructure and compliance with privacy by service providers.

Additionally, the focus group session revealed the following specific security and privacy concerns of respondents loss of control over data and privacy. SaaS application service providers do not have any legal obligations in Nigeria and therefore are not liable to prosecution, respondents indicated the need for a means of compliance to achieve more traceability.

Finally, respondents indicated they were hopeful that SaaS security improvements would have a significant impact on their decision-making process regarding the adoption of SaaS applications. Participants also indicated that they were planning organisation-wide adoption and alignment of SaaS applications.

5.5 Multi-tenant Access Control Barrier

5.5.1. Questionnaire Data

Tan *et al.* (2011) described a multi-tenant environment as having multiple customers or users who do not see or share each other's data but can share resources or applications in an execution environment even if they do not belong to the same organisation. This results in the optimal use of hardware and data storage mechanisms. The authors suggested that SaaS providers ensure separate data segregation at the physical and application levels to improve control access. Surya *et al.* (2013) described data segregation in SaaS applications as a situation where different users' data are hosted on the same data infrastructure.

Based on the above, the researcher asked whether SaaS application providers offer evidence of access control in a multi-tenant environment to ensure that users access only the portion of the application they are authorised to access.

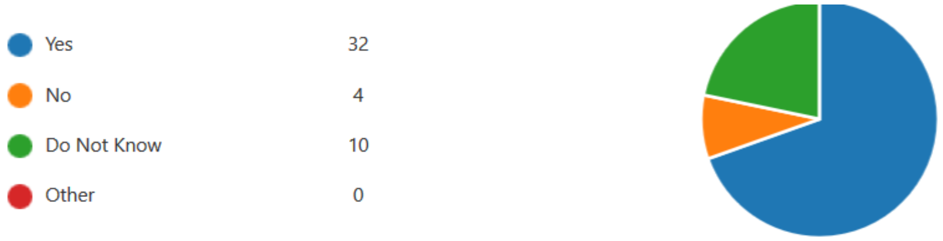


Figure 18: Multi-tenants and access control

As seen in Figure 18, 70% of respondents said their service provider offered evidence of access control and that access to SaaS applications was controlled according to the provisions of the SLA, 22% said they did not know, and 9% said their service provider did not offer such evidence.

From the responses, it can be inferred that while service providers claimed to offer evidence of access control in the SLA, the respondents could not verify this because of a lack of means for ensuring compliance with the textual obligations contained in the SLA.

5.5.2 Focus Group Data

Participants described multi-tenant access control concern as another primary concern during the focus group session when sharing the same hardware. They mentioned they are concerned with the attendant risks of unauthorised access to their data because of multi-tenancy. Because of the SaaS model’s core architecture, participants feared another user of the same hardware might be able to maliciously access another user's application data on the same device. They unanimously agreed that a tool that can help verify and grant access rights based on their preferences would be handy.

5.6 Data Location Barrier

5.6.1 Questionnaire Data

The location of data is another of the significant challenges SaaS applications face (Tiwari, Joshi 2014a). SaaS application data and the application itself are hosted on the service provider’s infrastructure, raising several security challenges. Georgios *et al.* (2017) investigated the impact of data locality via simulation on SaaS applications' performance, where real-time, data-intensive tasks are scheduled dynamically, under various data availability conditions.

To reduce the mismanagement of data, the GDPR requires the location of personal data of EU citizens to be warehoused within the EU's borders; organisations that fail to comply will be penalised. This presents a significant compliance challenge to SaaS application providers, users, and governments. (Subashini, 2011) highlighted this challenge and suggested that a secure SaaS model must be reliable and must provide information to the customer on the location of the consumer’s data. According to (Abuhussein, et al. 2012), knowing where the location of the server where the consumer data resides is essential. Consumers should make sure that their service providers do not expose information about the storage location.

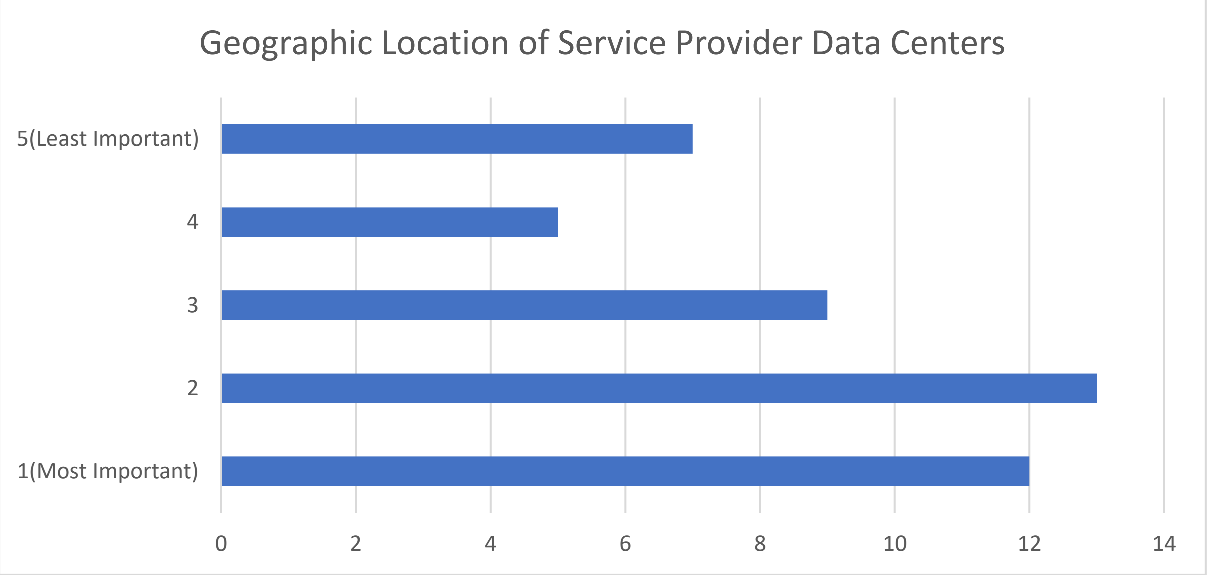


Figure 19: Geographic location of data

According to Figure 19, 54.4% of the respondents considered the service provider’s data centre's geographic location as a barrier to SaaS adoption. 26.1% considered it the most critical barrier, and 28.3% considered it a crucial barrier. A total of 19.5% of the respondents neither agreed nor disagreed that it was a barrier, and 10.9% said it was unimportant. Only 15.2% of the respondents said it was the least significant barrier to their SaaS adoption efforts.

5.6.2 Focus Group Data

Data location and control emerged as a theme in the focus group data. Participants reiterated that because of the concept of data sovereignty, they were pushing for a similar regulation such as the GDPR for keeping all data generated within Nigeria warehoused in Nigeria. The NITDA was advocating this. This regulation would oversee the movement of data hosted within the country. Participants expressed hope that this would spur interest in developing local infrastructure for data storage and help drive application service providers to host their applications within Nigeria.

5.7 Compliance Verification

5.7.1 Questionnaire Data

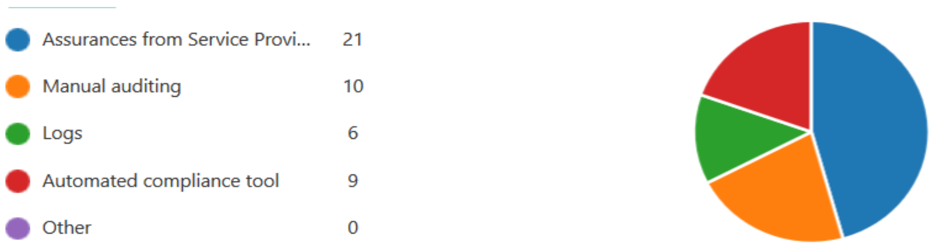


Figure 20: Compliance verification

Figure 20 above shows that 80.5% of the respondents said they verify compliance from assurances, manual auditing, and logs. A breakdown shows that 45.6% verified compliance from the SaaS provider's assurances, 21.7% verified it using manual auditing, and 13.2% verified it using logs acquired for monitoring purposes. Only 19.5% of the respondents said they used some limited automated means such as propriety tools from service providers (e.g. Microsoft Security Compliance Toolkit) (Baumgarten, et al. 2014) to verify compliance. This justified the need for automation of security and privacy compliance tools.

5.7.2 Theme 1: Compliance Tools

Participants discussed compliance tools, regulations, and frameworks and mentioned how they ensure compliance. They explained that they used SLAs to ensure compliance, but they did not use any tool to verify conformance with SLA provisions. One of the participants said they aligned their infrastructure and operations with ITIL and PRINCE2 and were considering relevant frameworks designed for the cloud in preparation for the eventual adoption of SaaS application across their operations. They expressed a unanimous desire for an automated means of verifying compliance with their SLA provisions.

5.7.3 Theme 2: Security Concerns

Participants indicated they were hopeful that SaaS applications' security would improve and that this would significantly affect their decision-making process regarding the adoption of SaaS. Participants also indicated they were planning broad adoption and alignment of software-as-a-service into their operations. They were optimistic that if appropriate specific controls were automated, especially about existing regulations, this would help drive their adoption and reduce security concerns.

5.7.4 Theme 3: Privacy Concerns

Participants indicated they were concerned about personal data privacy and about how SaaS application service providers handle it. Personal data and personally identifiable information were collected and could be used without the owners' consent. Participants stated that if a means were devised to verify how service providers handle their data based on their privacy preferences, it would improve their trust and confidence in SaaS applications and increase adoption.

5.7.5 Theme 4: Data Control

Participants reiterated that because of data sovereignty requirements, they were also pushing for a similar regulation such as the GDPR for keeping all data generated within Nigeria warehoused in Nigeria through the NITDA was advocating this. This regulation would cover all data hosted within the country. They also expressed hope that this would spur interest in local infrastructure for data storage and drive application service providers to host their applications within Nigeria.

5.7.6 Theme 5: Adoption of SaaS and Multi-tenant Access Control

Focus group participants reported that their SaaS application adoption decisions were influenced by concerns about regulations and their impact on data hosted outside Nigeria. Another major concern participants mentioned is sharing the same hardware and the attendant risks of having unauthorised access to their data due to multi-tenancy. Because this was the SaaS model's core architecture, they feared that a user on the same hardware would be able to maliciously access another user's application data on the same device. They unanimously agreed that a tool that could help verify and grant access rights based on their preferences would be relevant.

5.8 Conclusion of Result Analysis

First, findings from the two sources were triangulated and analysed as suggested by (Bryman 2004) and were independently analysed, and the results revealed that organisations are very interested in SaaS applications, with 92.2% indicating interest. However, due to the privacy of personal data usually collected by SaaS application providers, they are very concerned about compliance with privacy and data protection regulations. Interestingly, participants have reported it is a significant barrier and concern; this is evident, with 65% of respondents considering it an effective deterrent and needing a solution. The researcher was surprised to learn that was following similar study findings such (Brodin 2019b, Nagar et al. 2018b)

On data security, 71.9% of respondents indicated that it is a critical barrier to adopting SaaS applications in their organisation compared to other issues such as reliability, interoperability, and performance. While in the context of this research, security refers to the broad policies, controls, technologies, and solutions implemented to secure resources such as SaaS applications. It should not be confused with the privacy concept, which is mainly concerned with the privacy of data, particularly personal data. However, it is a critical concern and therefore relevant to the research.

On Multi-tenancy, which is a significant concern to users due to data privacy in SaaS applications, the participants concur that the integrity of their data is in question where they share hardware and application features with other users. This concern is expressed by 70% of respondents who further indicated that they could not verify that their data privacy is guaranteed since every user has access to SaaS applications. Additionally, they noted that they could not control who accesses the service as it is the responsibility of the Service provider, and it is based according to the SLA's provisions which are textual and from the perspective of the Service provider, thus protecting the interests of the service provider as argued by (Chen, et al. 2015)

On location of data, many times it has been reported to be a significant source of concern to organisations (Zissis, 2012, Skendžić, Kovačić et al. 2018). Additionally, it is a major requirement of the NDPR and even GDPR compliance. Organisations are legally required to locate or host their data within the jurisdictions where such regulations apply. The questionnaire outcome indicated 54.4% of that where their personal and operation data had kept a barrier to their SaaS adoption journey; this is further highlighted in the themes that emerged in the thematic analysis of the focus group session.

Finally, the ability to verify that SaaS applications service providers comply with data protection regulations has been the primary concern for organisations. Pieces of evidence in the literature review and field data have proved that users of SaaS applications may not verify if a service provider is complying with the provisions of a data protection regulation because they lack the tools or mechanisms that can empower them to do that. When asked how they currently verify data protection compliance, a majority of about 80.5% of respondents said they currently verify compliance based on the provider's assurances or by relying on manual auditing, which is not the true reflection of actual compliance. Additionally, 47.2% of respondents indicated that SaaS application service providers did not share any actionable information regarding vulnerabilities, breaches, and threats and other issues relating to compliance with them. Additionally, the participants overwhelmingly indicated that the automation of compliance with data protection regulation may empower them and encourage their adoption strategy, they unanimously agree that automation can help improve the transparency and traceability of compliance efforts.

These findings have led to the identification of some specific requirements at each stages the data life cycle that are encoded into privacy and data protection compliance sub-policies of the semi—formal policy language within the context of SaaS applications. They are as follows

I. Requirement 1: Data collection sub-policy
II. Requirement 2: Data processing sub-policy
III. Requirement 3: Data storage sub-policy
IV. Requirement 4: Data retention sub-policy
V. Requirement 5: Data forwarding sub-policy

5.9 Chapter Summary

This chapter discussed the results of the data collection and analysis methods. The data collection's objective was to understand the security, privacy, and data protection concerns of the organisations participating in the exercise. Furthermore, the chapter discussed data visualisations from the questionnaires and themes from the focus group. These findings were used to understand concerns expressed by respondents relating to SaaS application adoption.

The findings indicated that there is a strong interest in SaaS applications. However, respondents had concerns relating to regulatory compliance, their data security with a third party, their data privacy and integrity, jurisdictional control over their data, and the sharing of the same hardware with other users in a multi-tenant architecture.

Another significant finding was that respondents did not have any mechanism for checking compliance with privacy and data protection regulations. Additionally, the respondents and focus group participants indicated that they verified compliance based on SLAs signed with SaaS providers. Data analysis of their responses on compliance indicated that about 80.5% of the respondents checked for compliance with data protection regulations based on the provider's assurances or manual auditing of compliance procedures within their operations.

In the next chapter, these concerns will be mapped and aligned to the privacy and data protection principles of the NDPR.

CHAPTER SIX

6.0 SaaS-PPL

6.1 Introduction

In this chapter, the SaaS-PPL specification language is presented as extensions, logic, syntax, and semantics for reasoning about security, privacy, and data protection alongside evaluating the PPL. The logic is motivated by the principles of PbD and the end-to-end concept of the data life cycle (Butin, Métayer 2015) and (Vinh, 2018). The syntax is based on PPL's syntax, where an obligation is expressed using the Trigger–Action pair. Triggers are events related to obligations and conditions designed to fire actions by the data controller. Furthermore, semantics is based on PPL's structure, and it is expressed using semi-formal methods and logic. This systematic development of the language avoids the ambiguous semantics that has plagued other privacy languages.

Overall, the chapter answers the fourth research question on how to model compliance check syntax and shows proof of compliance when all properties are matched and validated within the context of SaaS applications.

6.2 PPL

According to (Trabelsi, et al. 2011), PPL was developed under PrimeLife project2 as an extension of XACML and similar languages such as XACML (OASIS 2017) and P3P (Olurin, et al. 2012). It allows for privacy-preserving access control using application-independent certified credentials for access authorisation based on credentials such as RBAC (Wang, et al. 2018) and ABAC (Daibouni, et al. 2016). PPL provides the additional benefit of regulating the use of personal information in secondary applications. It presents an obligation framework as an application layer platform in a distributed-service-oriented environment to enforce a service provider or data controller’s obligations to cater to a user or a data subject’s privacy needs. This sets it apart from previous policy languages that only provided minimal obligation capability and did not provide any concrete model for obligation specification.

6.2.1 Terminologies of PPL

Table 7: Terminologies of PPL

S/N	Terminology	Meaning
1	**Access Control**	This refers to controlling access to resources such as web pages, based on the identity of the entity requesting access, or more generally on the presentation of a set of credentials and representation of the purpose of accessing the resource, as well as other contextual information, such as the time of day and the properties of the resources themselves.

2	**Credentials**	A credential is an attestation of qualification, competence, or authority issued to an individual by a third party with a relevant de jure or de facto authority or assumed competence to do so.
3	**Personal Data**	Personal data means any information relating to an identified or identifiable natural person or ‘data subject’. An identifiable person can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural, or social identity.
4	**Data Controller**	This means the entity that alone or with others determines the purposes and means of personal data processing.
5	**Downstream Data Controller**	When a data controller passes personal data to a third party, that third party incurs obligations regarding the data subject and is referred to in this document as a ‘downstream data controller’.
6	**Data Subject**	The data subject is the person whose personal data are collected, held, or processed by the data controller.
7	**Data Subject’s Privacy Preferences**	This refers to the expectations of a data subject in terms of how his or her data should be handled.
8	**Authorisations and Obligations**	The data subject authorises the data controller to process their data, subject to the data controller meeting the obligations agreed upon with the data subject. PPL is a means for data controllers to define policies that describe proposed obligations and pass them on to the data subject for matching against their preferences.
9	**Sticky Privacy Policy**	This is an agreement between the data subject and data controller on the handling of personal data collected from the data subject. Sticky policies (as well as privacy preferences and privacy policies) define how data may be handled. Different aspects are defined, such as authorisations and obligations. • **Authorisations** refer to what a data controller is allowed to do with the collected data and the conditions under which the data controller is allowed to share data with a third party. • **Obligations** refer to the responsibilities of the data controller.
10	**User Agent**	This is a software system (such as a web browser) acting on behalf of a user. The user agent relies on user preferences when dealing with a server and acts on behalf of the data controller.
11	**Data Handling Policy Preference**	This is a policy configuration that states the usage conditions and conditions for handling targeted data. It refers to how the data controller will handle the collected data. The data subject will specify how their data should be handled after being collected.

(Trabelsi, et al. 2011), and (Azraoui, et al. 2015b)

The researcher extended the policies of data handling by creating extensions for service provider privacy obligations and user privacy preferences that the obligations engine will match to achieve data protection compliance.

6.2.2 PPL Architecture Components

The high-level architecture below presents an abstract overview of the PPL architecture and the interaction between the different entities: DS, DC, and third parties.

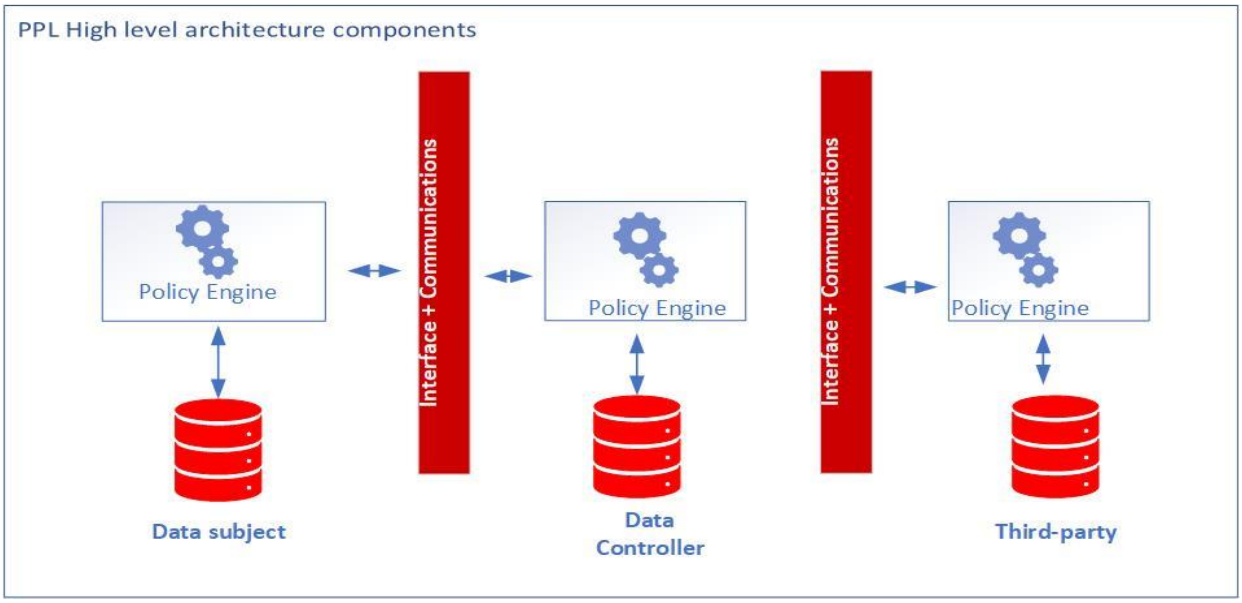

PPL High level architecture components
Policy Engine
Interface + Communications
Policy Engine
Interface + Communications
Policy Engine
Data subject
Data Controller
Third-party

Figure 21: PPL High-level architecture *(Azraoui, et al. 2015b)*

6.2.2.1 Data Subject

- **Policy Engine:** This component is in charge of parsing and interpreting the data subject’s privacy preferences. It supports all of PPL capabilities (preferences, access control, data handling preferences (DHP), obligations, credentials). For this reason, this module is replicated on the data controller side and the third-party side.
- **Repository**: This refers to the data and policy repositories. It is a database containing data the data subject owns. These data may be composed of personal data, credentials, certifications, and other information used when interacting with the data controller

application. It also contains the policy files representing the data subject’s privacy preferences.

- **Interface and Communication**: This interface allows communication with the data controller implementing the message exchange protocol.

6.2.2.2 Data Controller

- **Policy Engine:** This component is the same as the one described in the Data Subject section.
- **Repository**: This repository represents a database containing all information collected from the data subject during interaction sessions. These data represent personal data, credentials, certificates, and other information the user has provided. The database also contains privacy policies related to different resources and services the data controller possesses and offers. The repository does not contain any information about the data subject (e.g. IP addresses, page visited).
- **Interface and Communication**: This interface allows communication with the data subject about implementing the message exchange protocol. In the downstream interaction between the data controller and a third party, it plays the role of the user interface, as described in the Data Subject section.

6.2.2.3 Third-party Data or Downstream Controller

All the components supported by these actors are the same as those described in the Data Controller section because the third party plays the role of a data controller in the data’s downstream usage.

6.3 PPL Contributions

PPL’s main contributions have been in five main areas:

- **Data Handling:** Two-sided data handling policies/preference with automated matching.
- **Credential-based Access:** Credential-based access control specifying access control conditions in terms of credentials that need to be presented.
- **Equilibrium or Symmetry:** A form of equilibrium or symmetry that considers personal data as a particular type of resource in its own right and that allows for the use of the same language on the data subject's side to express conditions before revealing data as on the data controller's side to specify which personal data need to be revealed to access which service and how those data will be treated.
- **Downstream Data Use:** Another significant contribution of PPL is that it provided a route for downstream personal data usage. In this context, personal data is a resource offered by the data controller to downstream data controllers or third parties based on the data subject or owner's specifications.
- **Event-based Obligations:** Lastly, PPL contributed by adding event-based obligations. This feature is enforced by the obligation engine with the combination Trigger/Action, based on events related to the obligation's execution.

These XACML extensions were added to support all the above features in the entities' local policies. However, as seen in recent PPL extensions, there are limitations to the roles of data subjects, data controllers, and downstream controllers. PPL also did not incorporate accountability requirements, as in the A-PPL and other recent extensions such as the CPPL.

6.4 Limitations of PPL

PPL was not primarily designed for capturing the data protection rules in the NDPR and other similar regulations such as the GDPR. Its syntax and semantics are not expressive enough to capture the properties of the NDPR. For example, PPL is solely intended to be used by the data controller to specify access and authorisation restrictions to the service provider’s resources using sticky policies (Neven 2010). Therefore, the PPL framework has not been used to specify and express data protection requirements against the requirements outlined in the NDPR.

Given the above limitations, this research presents in Section 6.6 a new privacy and data protection policy, SaaS-PPL, that extends the syntax and semantics of PPL at each stage of the data life cycle within the context of SaaS applications. The language adds new semi-formal rules for a more fine-grained compliance check based on the new syntax and semantics. SaaS-PPL will rely on the PPL architecture to express its requirements. Furthermore, the language presents a semi-formal approach to applying SaaS-PPL for the end-to-end protection of personal data across the entire data life cycle within the context of SaaS applications.

There is no literature in the context of NDPR-compliant data security, privacy, and protection for SaaS applications to the best of the researcher's knowledge. The semantics and syntax of the proposed policy language for specifying compliance requirements, such as the NDPR, make it versatile.

6.5 Example of a PPL Obligation and Trigger

As discussed in Section 6.2, PPL was proposed to specify machine-readable privacy policies by building on XACML (Ardagna, et al. 2010), using extensions, and defining a new syntax for obligation and authorisation. Within PPL (Jaatun, et al. 2017), an obligation is expressed using the Trigger–Action pair. An obligation can be defined as follows:

Do **Action** when **Trigger**

Triggers are events related to an obligation and are filtered by conditions (Azraoui, et al. 2015a). Triggers fire actions such as personal data collection performed by a data controller. Some examples of PPL triggers and actions are (see (Laurent et all 2010) for more examples):

a) Triggers = condition + event. For instance, the construct $TriggerPersonalDataDeleted$ (address, 7 days) means 7 days after the deletion of an address. This construct *TriggerPersonalDataAccessedForPurpose*(phone, {call}, 3 hours) means within three hours of using a phone number for calling purposes.

b) Actions (e.g., delete an address, anonymise name and address, notify Pete via email). Examples of action constructs are,

$$ActionDeletePersonalData(\{address\})$$

$$ActionAnonymizePersonalData(\{name, address\})$$

$$ActionNotifyDataSubject(email, \{Pete\})$$

Authorisation defines the actions that the data controller is allowed or forbidden to perform, such as (a) authorisation for usage purposes and (b) authorisation for data forwarding to third parties.

6.6 SaaS-PPL Extensions and Logic

As indicated earlier, the fundamental roles defined in PPL (see Section 6.2), namely, the data subject, data processor, data controller, and the third-party data controller, will be retained because they align with the NDPR. Further, the definitions of the syntax for the service provider policy, the data types supported by the service, and the sub-policy definitions for each of the service types for specifying and expressing data protection properties of the NDPR are presented. The work of (Vinh Thong

Ta May 15, 2018)[6] inspired the SaaS-PPL policy syntax specification. Finally, the policy language's syntax is defined and aligned to the data life cycle (B. Spasic, A. Th. RATH et al. 2018b) and presented below in **Table 6** and a summary of all extensions provided in the **appendix**.

6.6.1 SaaS-PPL Policy Definition

The SaaS-PPL policy can be adapted to any type of data controller, but in this context, the researcher assumes the data controller is the service provider with a set of finite services. Furthermore, the following assumptions are made:

- Assuming the service provider supports the following sets of data types, typeset={θ_1,....,θ_2, θ_n}, where θ is a single data type $typeset1, \dots, typesetk$, (e.g. θ_1 = name). Two typesets do not have a common element, and their union is the set of all types supported by the service.
- A finite set $\{\mathrm{typeset}1, \dots., \mathrm{typeset}m\}$ that is supported by the service for all the data types supported by the service provider information.

Therefore, the data protection policy for the service is defined as follows:

$$Pol = (Pol\_typeset1, \dots, Pol\_typesetk)$$

Pol is the policy of the service provider's full service while *typesets* are sets that do not have common elements. When put together in a union of sets, they give the entire set of data types that are supported by the service. In this study, $typesets$ were considered instead of types. There can be a large set of types, allowing policies to be defined as a set. Thus, allowing policies not to be treated differently saves time. Individual types will have to be considered individually.

Additionally, having a set of types help in avoiding duplication of elements in the sub-policies. Therefore, the proposed end-to-end policy language enables a fine-grained privacy and data protection specification for compliance purposes at each stages of the data life cycle (Butin, Métayer 2015), consistent with the provisions of the NDPR and based on the service provider and user preferences.

6.6.1.1 Service Provider Preferences

The service provider and user preferences can be defined as follows:

- Service provider preferences are data handling obligations imposed by privacy and data protection regulations, such as the NDPR.
- User (or data subjects') preferences are specific preferences for their data to be processed (Azraoui, Elkhiyaoui et al. 2015a).

Therefore, a policy is defined for each data typeset. $Pol\_\mathrm{typeset} = (Pcol,\ Puse,\ Pstr,\ Pret, Pfw)$, therefore having $Pol = \{P\mathrm{ol\_typeset1}, \ldots, P\mathrm{ol\_typesetk}\}$, where $\mathrm{typeset1}, \ldots\ \mathrm{typesetk}$ are different sets of types (no common element)

1	$Pol\_\mathrm{typeset}.Pcol$	Denotes a reference to the collection policy for types in $typeset$.
2	$Pol\_\mathrm{typeset}.Pproc$	Denotes a reference to the usage policy for types in $typeset$.
2	$Pol\_\mathrm{typeset}.Pstr$	Denotes a reference to the storage policy for types in $typeset$.
4	$Pol\_\mathrm{typeset}.Pret$	Denotes a reference to the retention policy for types in $typeset$.
5	$Pol\_\mathrm{typeset}.Pfw$	Denotes a reference to the forwarding policy for types in $typeset$.

6.6.1.2 User or Customer Preferences

Here, like in the service provider preferences section, a finite set $\{typeset1, \dots . , typesetm\}$ is assumed for all the data types that are supported and preferred by the user. It is also assumed that the user or data owner agrees about the preferences of the service provider about the following sets of data types: $typeset1, \dots , typesetk$. Therefore, the user requirements and policy preferences for the service provider obligations are defined as follows:

$$REQ \ = \{R\_typeset1, \dots , R\_typesetk\},$$

User preferences are defined for each data type, $R\_typeset$ = ($Rcol$, $Ruse$, $Rstr$, $Rret, Rfw)$, so $REQ \ = \{R\_typeset1, \dots , R\_typesetk\},$ where $typeset1, \dots , typesetk$ is a different set of types (no common element).

1 $R\_typeset.Rcol$ Denotes the preference of the user about the collection policy of the service provider for typeset $typeset$.

2 $R\_typeset.Rproc$ Denotes the preference of the user about the processing policy of the service provider for typeset $typeset$.

3 $R\_typeset.Rstr$ Denotes the preference about the storage policy of the service provider for typeset $typeset$.

4 $R\_typeset.Rret$ Denotes the preference about the retention policy of the service provider for typeset $typeset$.

5 $R\_typeset.Rfw$ Denotes the preference about the forwarding policy of the service provider for typeset $typeset$.

6.6.2 SaaS-PPL Syntax of Sub-policies and Definitions

In accordance with the policies and preferences in the sections above, a set of data protection sub-policies is defined $(Pol\ )$ based on the end-to-end data life cycle (Suen, Ko et al. 2013, B. Spasic, A. Th. RATH et al. 2018b). Namely, this is a set of data collection sub-policies ($Pcol$), data processing sub-policies ($Pproc$), data storage sub-policies ($Pstr$), data retention sub-policies ($Pret$), and data forwarding sub-policies (Pfw).

Table 8: Policy sets

POLICY SETS ALIGNED TO DATA LIFE CYCLE

Data life cycle	Policy definition expression
Data collection	$Pcol$
Data processing	$Pproc$
Data storage	$Pstr$
Data retention	$Pret$
Data forwarding	Pfw

These sub-policies are formally defined as:

$$Pol = (Pcol, Pproc, Pstr, Pret, Pfw)$$

$$1.\, Pcol = (cons, cpurp)$$

$$2.\, Pproc\ (cons, procpurp, whocanproc, notify)$$

$$3.\, Pstr = (wherestore, howstore, notify)$$

$$4.\, Pret = (placeret, when, notify)$$

$$5.\, Pfw = (cons, fwpurp, 3rdparty, notify),$$

- The data collection sub-policies $Pcol$ includes consent required $(cons)$, which specifies the consent collection element. The consent collection element can be either Y (YES) or N (NO) for specific data types such as personal data and data collection purposes ($cpurp$).

- Processing policy is specified as $Pproc$ and requires consent to be collected before data processing and specified as ($cons$). The element for data processing purpose is specified as ($procpurp$), and the set of organisations that can process the data is specified as ($whocanproc$). Finally, the notification element is specified as $notify$, which captures whether the user or client needs to be notified before the processing of the data.
- The data storage policy is specified as $Pstr$, data storage is specified as $wherestore$, how the data are stored is specified as $howstore$, and notifications are specified as $notify$ to capture whether the user or client needs to be notified before the storage of the data.
- The data retention policy is expressed as $Pret$, the location where the data are retained is expressed as $placeretdecl,$ the time when the data are retained is expressed as $when$, with $when$ = ($rdelay = dd$) for defined retention periods and $when$ = ($gdelay = gd$) for worst-case retention delays. Here, notifications are specified as $notify$ to capture whether the user or client needs to be notified before deleting the data.
- The data forwarding policy Pfw involves collecting consent, specified as $cons$, and the requirement for forwarding purpose, specified as $fwpurp,$ as well as a set of third-party organisations or third countries to which the data will be forwarded, specified as $3rdparty$. Furthermore, $notify$ expresses whether the user or client needs to be notified before transferring the data.

Each sub-policy element is further defined as follows:

- $Pcol = (cons, cpurp), with\ cons\ \in \{Yes, No\}$. Here, consent is required to be obtained from users when collecting their data and specified as Y (YES) and N (NO). $cpurp$ = ($Pol\_typeset.Pcol$, *decl*) $Pol\_typeset.Pcol$ represents the data collection policy for the types $typeset$.
- $Pproc(cons, procpurp, whocanuse, notify)$. Here, the sub-policy for processing is specified, and consent is required to process personal data, denoted as $cons$. The processing purpose $procpurp$ and $whocanuse$ denote who is allowed to use the data, including third-party entities. Finally, $notify \in \{Y, N\}$, which denotes whether notification is required *(Y)* or not *(N)* before any data processing.

  $Pstr = (wherestore, howstore, notify)$, $where\ decl \in \{Y, N\}$.Here the researcher proposes a policy for data storage specifying where data are stored, denoted as $wherestore$, and how data are stored, $howstore$. $wherestore$ denotes a set of places where the *data* are stored, such as in the service provider's $(SPstorage)$ servers. $wherestore \in \{(SPstorage, 3rdpartyStorage, decl)\}$ $howstore$ = (Available, Hidden) denotes that the data are encrypted with the service provider's key and content is available to the service provider ($howstore$ = 'available'). *decl* specifies the declaration of this information to users. Finally, $notify\ \in\ \{Y, N\}$.
- $Pret = (placeret, when, notify)$, where $notify\ \in\ \{Y, N\},)$. Here, the researcher specifies $placeret$ as a set of elements ('$mainstorage$', '$backupstorage$', '$3rdparty$'). $when$ = ($rdelay = dd$) denotes a numerical retention delay value.
- $Pfw = (cons, fwpurp, 3rdparty, notify, decl)$, $where\ decl \in \{Y, N\}$, $cons$ = *{Y, N},* The policy for data forwarding requires consent for data forwarding purposes, denoted as a list of forwarding $fwpurp$,

a list of $3rdparty$ elements, and a notification element expressed as $notify \in \{Y, N\}$ This takes the *Y (YES)* or *N (NO)* value to capture whether the user or client needs to be notified before the data are forwarded.

6.6.3 Obligations

Obligations are a service provider's commitment to a user or data subject concerning handling the user's data. They usually refer to the requirements or provisions of a data protection regulation such as the NDPR. The service provider is expected to meet the obligation by implementing an action after a particular event, for example, time, and optionally under certain conditions. Furthermore, obligations are essential because they help ensure that the commitments made by the service provider are kept in compliance with data protection regulations or preferences of the data subject.

6.6.3.1 Utility and Challenges of Obligations

Obligations play an important role in service providers' responsibilities because service providers collect personal data and use state-of-the-art mechanisms for handling the data. Privacy and data protection regulations lack expressiveness and support for the definition of obligations. Key challenges service providers face related to obligations include:

- Service providers must avoid committing to obligations that cannot be enforced. Tools to detect inconsistencies are therefore necessary.
- Service providers should offer a way to take the user's preferences into account. This will make mechanisms to compare the user's privacy preferences and the service provider's privacy policies necessary.

- Service providers need a way to communicate acceptable obligations to users, link obligations and personal data, and enforce obligations.
- Finally, users need a way to evaluate service providers' trustworthiness, such as whether the obligation will indeed be enforced by audit and certification mechanisms and whether computers and tools can be relied upon.

Therefore, in this research, relying on existing PPL, data protection properties are expressed as obligations in the form of extended triggers and actions. The obligation engine syntax as is a set of actions, such as a 'Do **Action** when a particular **Trigger** is called'.

The triggers represent events that are considered by an obligation and result in actions such as 'Do **Action** when **Trigger**'. Therefore, the primary obligation definition used in PPL is as follows: 'Do **Action** when **Trigger** and therefore, the researcher create new extensions into SaaS-PPL extensions'. The basic definition of obligation is further extended as 'When **Trigger**, then **Condition**'.

Additionally, because PPL was not primarily designed for capturing data protection rules in the NDPR, its syntax and semantics are not expressive enough to capture properties of the new NDPR. For example, PPL is solely intended to be used by the data controller to specify access and authorisations restrictions on the service provider's resources using sticky policies (Slim et al., 2010). Therefore, the PPL framework cannot be used to specify and express some of the privacy and data protection properties of the NDPR. For example, the NDPR introduced new novelties such as Article 25 requiring data minimisation, as well as other privacy by design novelties such as the right to erasure, collection of consent, transparency before data processing, transfer of personal data to another data controller, and notification of any personal data breach within 72 hours.

Therefore, bold letters are used to indicate action, and ‘Do **Action** when **Trigger’** is used to indicate extended Triggers and Actions.

6.6.4 Semantics of Data Protection Policies

Each data protection policy’s semantics will be presented to give meanings to expressions, statements, and program units (Gawanmeh, 2015). Obligations and their corresponding triggers and actions for each collection, processing, storage, retention, and forward phase will be presented.

6.6.4.1 The Semantics of the Collection Policy

The following is defined in the context of the data collection obligation for the data collection phase. $Pcol = (cons, cpurp), with\ cons\ \in \{Yes, No\}$. The NDPR (see Section 5.1.1) requires data controllers to make known their purpose before they collect personal data; it also requires them to know how they intend to process the data. Furthermore, to avoid data being collected arbitrarily, the regulation seeks to limit data collection to the purpose for which it is collected (NITDA, 2019). This is a new requirement that PPL is not designed to express.

6.6.4.2 **Case 1.0 Personal Data Collection-Consent Collection**

This is an event-based trigger. The trigger occurs each time personal data associated with the obligation are collected and consent of data owner and specified purpose.

Collection Trigger for Consent:

- $TriggerCollectPersonalData(typeset, time)$

Collection Action for Consent:

- $ActionCollectConsent(typeset, time - value)$

Collection obligation for consent:

- *Do* $\boldsymbol{ActionCollectConsent(typeset, time - tvalue)}$ $when$ $\boldsymbol{TriggerCollectPersonalData(typeset, time)}$

Figure 22: Trigger Consent collection

In Figure 22, the collection obligation for consent states that whenever there is a trigger that captures data of types in typeset at time $time$, there is a corresponding action consent collection (here*,* $time - tvalue$ specifies the minus operation, namely, $time$ minu*s* $tvalue$*).* The collection of consent before data collection helps ensure that data collection is strictly conducted in compliance with Article 25 of the NDPR.

6.6.4.3 **Case 1.1 Personal Data: Purpose of Data Collection**

In Figure 23, the trigger for purpose occurs each time personal data associated with an obligation are collected for a specified purpose from the subset of purposes for collecting personal data.

Collection Trigger for Purpose:

- $TriggerCollectPurposes(typeset, purposes)$

Collection ***Condition*** *for Purpose:*

- $SubsetOf\ (purposes, cpurp)$

Collection obligation for purpose:

- $When\ TriggerCollectPersonalData(typeset, purposes)$**,** *then* $SubsetOf\ (purposes, cpurp)$

Figure 23: Trigger for purpose collection

The collection obligation trigger for purpose denotes that whenever data are collected with the purpose $purposes$, then $purposes$ must be a subset of $cpurp$. The collection of purposes aims to fulfil the NDPR's mandate to minimise the collection of data to a specific purpose. This is because data minimisation is at the centre of the NDPR and the privacy by design requirement of the NDPR.

6.6.5 The Semantics of the Processing Sub-policy

In Section 2.1 (subsection (a)) of the NDPR, data controllers are requested to collect data according to a clear lawful purpose. This purpose is to be communicated and have the consent of the data subject. A service provider's policy should have indicated details on (i) consent for use, (ii) processing purpose, and (iii) who can use the data. These requirements are expressed as four elements to capture the data processing phase; they include $Pproc = (cons, procpurp, whocanproc, notify)$. These elements are each considered as obligations in the following figures cases for each element.

6.6.5.1 **Case 2.0 Personal Data Processing Consent Collection**

In this case, consent is provided and expressed as a Yes and expressed as $cons$ = Y beside any possible/defined value of $procpurp, whocanproc, notify$. Additionally, the data processing obligation says that whenever there is a trigger that captures a data processing of the data types in $typeset$ at time $time$, there is a corresponding action obligation for collecting a data processing consent before that.

Processing Trigger for Consent:

- $TriggerProcessPersonalData\ (typeset,\ time)$

Processing Action for Consent:

- $ActionProcessConsent\ (typeset,\ time\ tvalue)$

Processing obligation for consent:

- Do $ActionProcessConsent\ (typeset,$
  $time\ tvalue)\ when\ TriggerProcessData\ (typeset,\ time\ tvalue)$

Figure 24: Personal data processing obligation – Consent

Here, in Figure 24, the trigger for consent occurs each time the personal data associated with the data processing obligation is collected for the specified consent for collecting the personal data.

6.6.5.2 **Case 2.1 Personal Data Processing Purpose**

As mandated by data protection regulations, there must be a specific purpose for collecting and processing data. The processing purpose denotes that whenever there is data processing with $purposes$, then $purposes$ must be a subset of $procpurp$.

Processing Trigger for Purpose:

- $TriggerProcessPersonalData\ (typeset\ , purposes)$

Processing ***Condition*** *for Purpose:*

- $SubsetOf\ (purposes, procpurp)$

Processing obligation for purpose:

- $When\ TriggerProcessPersonalData\ (typeset\ , purposes),$
  $then\ SubsetOf\ (purposes, procpurp)$

Figure 25:Personal data processing obligation- purpose

6.6.5.3 **Case 2.2 Personal Data Processing whocanproc**

The processing obligation for $whocanproc$ captures that whenever organisations conduct data processing in the set $processby$, then $processby$ must be a subset of $whocanproc$.

Processing Trigger for $whocanproc$:

- $TriggerProcessPersonalData\ (typeset, processby)$

Processing Condition for $whocanproc$:

- $SubsetOf\ (processby, whocanproc)$

Processing obligation for $whocanproc$:

- $When\ TriggerProcessPersonalData\ (typeset, processby)\ ,$
  $then\ SubsetOf\ (processby, whocanproc)$

Figure 26: Personal data processing obligation whocanproc

6.6.5.4 **Case 2.3 Personal Data Processing – Notification**

When *($notify$ = Y),* besides any possible defined value of $cons, procpurp, whocanproc$.

The obligation for processing a notification means that whenever a type of data is processed in a typeset, the data subject must be notified at least $t - value$ time before the processing starts.

Processing Trigger for $Notification$*:*

- $TriggerProcessPersonalData\ (typeset, time)$

Processing Action for $Notification$*:*

- $ActionProcessNotification\ (typeset, time - tvalue\ )$

Processing Obligation for $Notification$:

- $Do\ ActionProcessNotification\ (typeset, time - tvalue\ )\ when$
  $TriggerProcessPersonalData\ (typeset, time - tvalue\ )$

Figure 27: Personal data processing obligation notification

6.6.6 The Semantics of the Storage Sub-policy

Subsection C of the NDPR mentions a policy relating to data storage within a reasonably needed period to store the data. In a situation where a specific type of data is held in storage by a data controller or SaaS service provider, (i) the location of storage must be known, (ii) the data must be in secure storage infrastructure, and (iii) a periodic review must be conducted of why the personal data are in storage. The storage phase is expressed as $Pstr = (wherestore, howstore, notify\ )$, $where\ notify \in \{Y, N\}$. The cases are distinguished depending on the values of each element or parameter.

6.6.6.1 Case 3.0 Personal Data Storage Obligation Encrypted

$If\ wherestore = \{SpOwnServer\}$, and $howstore = \{Available\}$)
Whenever there is action $TriggerStoreData\ (typeset,\ time)$, then there must be an action $ActionSaveEncryptedData$, where a type of data in $typeset$ is encrypted with the server key $spkey$ at the place(s) $SpOwnServer$.

Storage Trigger for how and where data is stored:

- $TriggerStoreData\ (typeset, time)$

Storage action for $wherestore$ and $howstore$:

- $ActionSaveEncryptedData\ (typeset, spkey, SpOwnServer, time)$

Storage obligation for where and how data is stored ($wherestore$, $howstore$):

- *Do* $ActionSaveEncryptedData\ (typeset, spkey, SpOwnServer, time)$ *when* $TriggerStoreData\ (typeset, time)$

Figure 28 Personal Data Storage Obligation-Save Encrypted with Service Provider Key

6.6.6.2 Case 3.1 Personal Data Storage Obligation – Saved in Plain Text

This case is like the previous case, but a type of data in $typeset$ is saved in plain text at the place(s) $SpOwnServer$. This is expressed as $If\ wherestore = \{SpOwnServer\}$ and $howstore = \{Available\}$)

Storage Trigger for how and where data is stored:

- $TriggerStoreData\ (typeset, time)$

Storage action for $wherestore$ and $howstore$:

- $ActionSavePlainData\ (\ typeset,\ SpOwnServer,\ time\ )$

***Storage** obligation for where and how data is stored ($wherestore$, $howstore$):*

- *Do* $ActionSavePlainData\ (\ typeset,\ SpOwnServer,\ time\ )$ *when* $TriggerStoreData\ (typeset, time)$

Figure 29:Personal data storage obligation-save plain data on the service provider server

6.6.6.3 Case 3.2 Personal Data Storage Obligation – *howstore* Hidden

$If\ wherestore = \{SpOwnServer\}$, and $howstore = \{Hidden\})$

Storage Trigger for how and where data is stored:

- $TriggerStoreData\ (typeset, time)$

Storage action for $wherestore$ *and* $howstore$:

- $ActionSaveEncryptedData\ (typeset, notspkey, SpOwnServer, time)$

Storage obligation for where and how data is stored ($wherestore,\ howstore$ *):*

- $Do\ ActionSaveEncryptedData\ (typeset, notspkey, SpOwnServer, time)$, *when* $TriggerStoreData\ (typeset, time)$

Figure 30:Personal Data storage obligation-save encrypted from a service provider

This case in Figure 30 depicts a scenario where a type of data in *typeset* is encrypted with a key that is not a service provider key; that is, the service provider does not have access to this key by default.

6.6.6.4 Case 3.3 Personal Data Storage Obligation – *howstore* Available

In this case, the service provider stores a type of data on the $3rdPartyServers$. The data are encrypted with a key, so the service provider has access to the data. This case is specified as ($wherestore = \{3rdPartyServers\}$, and $howstore = \{Available\})$

Storage Trigger for how and where data is stored:

- $TriggerStoreData\ (typeset, time)$

Storage action for $wherestore$ *and* $howstore$:

- $ActionSaveEncryptedData\ (typeset,\ spkey,\ 3rdPartyServers, time)$

Storage obligation for where and how data is stored ($wherestore,\ howstore$)

- $Do\ ActionSaveEncryptedData\ (typeset, spkey, 3rdPartyServers, time)$, *when* $TriggerStoreData\ (typeset, time)$

Figure 31: Personal Data Storage Obligation- Encrypted and Stored on 3rdParty Server by Service provider

6.6.6.5 **Case 3.4 Personal Data Storage Obligation – $\boldsymbol{howstore}$ Clientplace**

In this case, the service provider stores a type of data on the $3rdPartyServers$, which are encrypted with a key that is not accessible to the service provider and is expressed as $(wherestore = \{3rdPartyServers\}.\ howstore = \{Hidden\})$ when $wherestore = \{Clientplace\}$ can be further specified to denote when the data can be stored at the client's place.

Storage Trigger for and where data is stored:

- $TriggerStoreData\ (typeset, time)$

Storage action for $wherestore\ and\ howstore$:

- *ActionSaveEncryptedData (typeset, notspkey, $clientplace$, time)*

Storage obligation for where and how data is stored ($wherestore,\ howstore$)

- $Do\ ActionSaveEncryptedData\ (typeset, notspkey, clientplace, time), when$ $TriggerStoreData(typeset, time)$

Figure 32:Personal data storage obligation-save encrypted and stored on 3rdParty server

6.6.7 The Semantics of the Retention Sub-policy

Regarding data retention, Section 3.1 (9) in the NDPR has described the rights that data subjects can exercise regarding whether they would exercise their right to the retention or deletion of their data from a service provider's infrastructure. Therefore, by implication, service providers are required to create a mechanism or provisions for the enforcement of these rights by formulating policies relating to data retention. They need to pay particular attention to details such as (i) where a service provider can retain data, (ii) what type of data is allowed to be deleted or retained, and (iii) whether and until when the deletion can be delayed.

6.6.7.1 **Case 4.0 Case 4.1 Personal Data Retention – Notification**

In the data retention policy case, $Pret =$ $(placeret, when, notify)$, where $notify\ \in \{Y, N\},)$, $placeret$ is a set of elements describing retention of data (‘$mainstorage$’, ‘$backupstorage$’, ‘$3rdparty$’) and when = $(rdelay, gdelay)$ has the following semantics:

6.6.7.2 **Case 4.1 Personal Data Retention – Notification**

If $notify$ = Y, besides any $placeret$ and $when$ values.

Retention Trigger for Retention Notification:

- $TriggerRetentionPersonalData\ (typeset, time)$

Retention Action for Retention Notification:

- $ActionRetentiontionNotification(typeset, time - tvalue\ )$

Retention Obligation for Retention Notification:

- *Do* $ActionRetentionNotification(typeset, time - tvalue)\ when\ TriggerRetentionPersonalData\ (typeset, time)$

Figure 33: Personal Data Retention-Notification

Whenever a piece of data of the type in the set of types $typeset$ is deleted, then the data subject needs to be notified $tvalue$ time before that.

6.6.7.3 **Case 4.2 Personal Data Retention Obligation – Trigger Data Retention**

In $when$, $rdelay = dd$, besides any global delay ($gdelay$), where dd is a $numerical$ retention delay value, namely,

Retention Trigger for Data Retention:

- $TriggerInitiateRetentionData\ (typeset, time1)$

Retention Action for Data Retention:

- $ActionDataRetention(typeset, fromwhere, time2, [time1, time1 + dd])$

Retention Obligation for Data Retention:

- *Do* $ActionDataRetention(typeset, fromwhere, time2, [time1, time1 + dd])$
  $When\ TriggerInitiateRetentionData(typeset, time1)$

Figure 34: Personal Data Retention Obligation - Trigger Data Retention

$time2, [time1, time1 + dd]$ specifies the time $time2$ between $time1$ and $time1 + dd$.

6.6.7.4 **Case 4.3 Personal Data Retention Obligation - Global delay**

$when\ gdelay = gd$ is triggered whenever the user unregisters from the service and the data need to be retained within the global delay, *gd*.

Retention Trigger for Data Retention:

- $TriggerUnregister\ (typeset, time1)$

Retention Action for Data Retention:

- $ActionDataRetention\ (typeset, fromwhere, time2, [time1, time1 + gd])$

Retention Obligation for Data Retention:

- *Do* $ActionDataRetention(typeset, fromwhere, time2, [time1, time1 + gd])$
  $When\ TriggerUnregister\ (typeset, time1)$

Figure 35: Personal Data Retention -Retention Action for Data Retention

6.6.8 The Semantics of the Forwarding Sub-Policy

As services and service providers continue to depend on each other to provide services to users, the need to share data amongst service providers becomes critical. Therefore, to ensure effective regulation and data subjects' rights, data protection regulations require that for data forwarding to be permissible, consent must be obtained. In Sections 2.11 and 2.12 of the NDPR, the data forwarding criteria described what conditions must be met for a service provider or data controller to transfer personal data to a third-party recipient: (i) consent provided by the data subject, (ii) an explicit explanation for why the data will be forwarded, and (iii) a list detailing the recipients of the data.

6.6.8.1 **Case 5.0 Personal Data Forwarding Obligation – Consent**

For the data forwarding phase, where P$fw =$ $(cons, fwpurp, 3rdparty, notify\ )$, $where\ decl \in \{Y, N\}$, $cons$ = {Y, N}, the policy requires consent for data forwarding, denoted as ($cons$); a forwarding list, $fwpurp$; and a list of $3rdparty$ and notification, $notify \in$ $\{Y, N\},$ which takes the value of *Y (YES)* and *N (NO).*

Forwarding Trigger for Consent:

- $TriggerForwardPersonalData(typeset, time)$

Forwarding Action for Consent:

- $ActionCollectConsent(typeset, time - value)$

Forwarding obligation for consent:

- *Do* $ActionCollectConsent(typeset, time -$ $value) when\ TriggerForwardPersonalData(typeset, time)$

Figure 36: Personal Data Forwarding Obligation-Consent

In Figure 36, the forwarding obligation for consent indicates that whenever there is a trigger that captures a data forwarding of data of types in typeset at time $time$, there is a corresponding action consent collection, with $time - tvalue$ specifying the minus operation, namely, $time$ minus $tvalue.$

6.6.8.2 **Case 5.1 Personal Data Forwarding Obligation – Purpose**

The forwarding obligation for purpose captures that whenever there is a data forwarding with $purposes$, then $purposes$ must be a subset of $fwpurp$.

Forwarding Trigger for Purpose:

- $TriggerForwardingPurposes(typeset, purposes)$

*Collection **Condition** for Purpose:*

- $SubsetOf\ (purposes, fwpurp)$

*Forwarding obligation for purpose**:***

- $When\ TriggerForwardPersonalData(typeset, purposes)\ then$ $SubsetOf\ (purposes, fwpurp)$

Figure 37: Personal data forwarding obligation-forwarding purpose

6.6.8.3 **Case 5.2 Personal Data Forwarding Obligation – Third-party List**

The forwarding obligation for $3rdpartyForwarding$ denotes that whenever there is a trigger to forward data to $3rdPartyRecipien$t with the condition $3rdpartyForwarding$, then $3rdpartyForwarding$ must be a subset of $fw3rdparty$.

Forwarding Trigger for 3rdpartyForwarding:

- $TriggerForward3rdPartyRecipient\ (typeset, 3rdparty)$

*Forwarding **Condition** for 3rdpartyForwarding:*

- $SubsetOf\ (purposes, fwpurp, fw3rdParty)$

Forwarding obligation for 3rdParty forwarding:

- $When\ TriggerForwardPersonalData(typeset,)$,*then* $SubsetOf\ (purposes, fwpurp, 3rdParty)$

Figure 38: Personal data forwarding obligation-3rdParty recipient list

6.6.8.4 **Case 5.3 Personal Data Forwarding Obligation – Notification**

If $notify$ = Y, besides any $fwpurp$ and $when$ values.

Forwarding Trigger for Notification:

- $TriggerForwardPersonalData\ (typeset, time)$

Forwarding Action for Notification:

$ActionDeletionNotification\ (typeset, time - tvalue\ )$

Forwarding Obligation for Notification:

- *Do* $ActionForwardingNotification\ (typeset, time - tvalue)\ when\ TriggerForwardingPersonalData(typeset, time$

Figure 39: Personal data forwarding obligation-notification

6.7 User Preferences

6.7.1 User Preference $\boldsymbol{Rcol}$

User preference $Rcol\ = (cons, cpurp), with\ cons\ \in \{Yes, No\}$

6.7.1.1 Preference of User: $\boldsymbol{cons}$ = Y => Match with the Obligation

There is an expectation of the following obligation from the service provider side:

$$D\boldsymbol{o}\ \boldsymbol{ActionCollectConsent}\ (\boldsymbol{typeset}, \boldsymbol{time} - \boldsymbol{tvalue})\ \boldsymbol{when}\ \boldsymbol{TriggerCollectPersonalData}(\boldsymbol{typeset}, \boldsymbol{time})$$

Inconsistency can occur when the service provider, in $Pcol$, does not receive a corresponding obligation.$cons$ = N means no consent is provided for data collection in the following obligation:

$$Do\ \boldsymbol{ActionCollectConsent}(\boldsymbol{typeset}, \boldsymbol{time} - \boldsymbol{tvalue})\ when\ \boldsymbol{TriggerCollectPersonalData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.1.2 Preference of User Collection Purpose $\boldsymbol{cpurp}$

This means that there must be a collection of purpose Trigger that initiates clarification of the purpose of data collection by the service provider.

$$When\ \boldsymbol{TriggerCollectPersonalData}\ (\boldsymbol{typeset}, \boldsymbol{purposes}), then \\ \boldsymbol{SubsetOf}\ (\boldsymbol{purposes}, \boldsymbol{cpurp})$$

6.7.2 User Preferences $\boldsymbol{Rproc}$

User preferences $Rproc$ = $(cons, procpurp, whocanproc, notify)$.

6.7.2.1 Preference of User: $\boldsymbol{cons}$ = Y => Match with the Obligation Trigger to Process Personal Data

This means that there is an expectation that the service provider will obtain the user’s consent for the processing of personal data:

$$Do\ \boldsymbol{ActionProcessConsent}(\boldsymbol{typeset}, \boldsymbol{time} - \boldsymbol{tvalue})\ when \\ \boldsymbol{TriggerProcessData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.2.2 Preference of User for the Purpose of Data Processing $\boldsymbol{procpurp}$

The processing purpose $procpurp$ Trigger obligation denotes that the service provider must meet the obligation for purposes before processing personal data whenever there is a data processing.

$$When\ \boldsymbol{TriggerProcessPersonalData}(\boldsymbol{typeset}, \boldsymbol{purposes}), then \\ \boldsymbol{SubsetOf}\ (\boldsymbol{purposes}, \boldsymbol{procpurp})$$

6.7.2.3 Preference of User Regarding Who Can Process Personal Data $\boldsymbol{whocanproc}$

This user preference is for the service provider to know who is allowed to process the user’s personal data. The Trigger obligation for whocanproc denotes that whenever the service provider conducts data processing, users are obligated to know who has the right to process their personal data.

$$When\ \boldsymbol{TriggerProcessPersonalData}(\boldsymbol{typeset}, \boldsymbol{processby}), then$$
$$\boldsymbol{SubsetOf}\ (\boldsymbol{processby}, \boldsymbol{whocanproc})$$

6.7.2.4 Preference of User Regarding Who Can Process Personal Data $\boldsymbol{notify}$

The trigger obligation for notification $notify$ denotes that when the service provider processes personal data, such as in a data breach situation, there is an expectation to notify the user or data owner.

$$Do\ \boldsymbol{ActionProcessNotification}(\boldsymbol{typeset}, \boldsymbol{time - tvalue})\ when$$
$$\boldsymbol{TriggerProcessPersonalData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.3 User Preferences $Rstr$

User preferences $Rstr$ =($wherestore, howstore, notify$).

6.7.3.1 Preference of Users for $\boldsymbol{Wherestore}$

This means that the user expects the service provider to have an obligation to encrypt and store personal data using the service provider's encryption keys. The user will have access to the keys.

$$Do\ \boldsymbol{ActionSaveEncryptedData}(\boldsymbol{typeset}, \boldsymbol{spkey}, \boldsymbol{SpOwnServer}, \boldsymbol{time}), when \\ \boldsymbol{TriggerStoreData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.3.2 Preference of User for $\boldsymbol{howstore}$

This means that the user expects the service provider's side to store the data in plain text in their server. Storage obligation for where and how data are stored ($wherestore, howstore$):

$$Do\ \boldsymbol{ActionSavePlainData}(\boldsymbol{typeset}, \boldsymbol{SpOwnServer}, \boldsymbol{time}), when \\ \boldsymbol{TriggerStoreData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.3.2.1 ($\boldsymbol{wherestore} = \{\boldsymbol{SpOwnServer}\}$, and $\boldsymbol{howstore} = \{\boldsymbol{Hidden}\}$)

Here, the user preference is for the service provider to store the data on their storage platform or servers, but not with the service provider's keys. This means the data will be hidden from the service provider by default. Storage obligation for where and how data are stored ($wherestore, howstore$):

$$Do\ \boldsymbol{ActionSaveEnctyptedData}(\boldsymbol{typeset}, \boldsymbol{notspkey}, \boldsymbol{SpOwnServer}, \boldsymbol{time}), when \\ \boldsymbol{TriggerStoreData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.3.2.2 $(\boldsymbol{wherestore} = \{\boldsymbol{3rdPartyServers}\}$, and $\boldsymbol{howstore} = \{\boldsymbol{Available}\})$,

Here, the user preference is to have the personal data stored on a third-party infrastructure and encrypted with the service provider's key that is made available to the service provider by default. Storage obligation for where and how data are stored $(wherestore, howstore)$:

$$Do\ \boldsymbol{ActionSaveEncryptedData}\ (\boldsymbol{typeset}, \boldsymbol{spkey}, \boldsymbol{3rdPartyServer}, \boldsymbol{time}), when\ \boldsymbol{TriggerStoreData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.3.2.3 $(\boldsymbol{wherestore} = \{\boldsymbol{3rdPartyServers}\}$, and $\boldsymbol{howstore} = \{\boldsymbol{Hidden}\})$

Here, the user preference is to have the service provider store the user's personal data on a third-party infrastructure with encrypted keys but are not accessible by the service provider. Storage obligation for where and how data is stored $(wherestore, howstore)$:

$$Do\ \boldsymbol{ActionSaveEncryptedData}(\boldsymbol{typeset}, \boldsymbol{notspkey}, \boldsymbol{3rdPartyServer}, \boldsymbol{time}), when\ TriggerStoreData(typeset, time)$$

6.7.3.3 User Storage Preference for Notification: $\boldsymbol{notify}$

This user expects the service provider to send a notification to the user if their personal data are about to be stored. Storage obligation for notification:

$$Do\ \boldsymbol{ActionStoreNotification}(\boldsymbol{typeset}, \boldsymbol{time} - \boldsymbol{tvalue})\ when\ \boldsymbol{TriggerStorePersonalData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.4 User Preference $\boldsymbol{Rret}$

User preference $Rret\ = (placeret, when, notify), where\ notify\ \in \{Y, N\})$.

6.7.4.1 Preference of User for Personal Data Retention

Under this policy, the user or data owner expects the service provider to have an obligation to notify the data owner when retaining personal data in specific storage types and locations over a specific period.

6.7.4.2 Preference of user for retention notification $\boldsymbol{placeret}$

Here, the user preference is for the service provider to notify the user when personal data in the set of types typeset for retention are triggered. The data subject needs to be notified $t - value$ time before that. Retention obligation for retention notification:

$$Do\ \boldsymbol{ActionRetentionNotification}(\boldsymbol{typeset}, \boldsymbol{time} - \boldsymbol{tvalue})\ when\ \boldsymbol{TriggerRetentionPersonalData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.4.3 Preference of User Retention Delay Decision $\boldsymbol{when}\ (\boldsymbol{rdelay})$

$when = (rdelay)\ rdelay$ refers to a delay in retention decision, that is, $when$, $rdelay = dd$, besides any global delay $(gdelay)$, where dd is a *numerical* retention delay value, namely, $time2, [time1, time1 + dd]$ specifies the time $time2$ between $time1$ and $time1 + dd$. Retention obligation for data retention:

$$Do\ \boldsymbol{ActionDataRetention}(\boldsymbol{typeset}, \boldsymbol{fromwhere}, \boldsymbol{time2}, [\boldsymbol{time1}, \boldsymbol{time1} + \boldsymbol{dd}])\ When\ \boldsymbol{TriggerInitiateRetentionData}(\boldsymbol{typeset}, \boldsymbol{time1}).$$

6.7.4.4 Preference of User Retention Delay at Global Level $\boldsymbol{when}\ (\boldsymbol{gdelay})$

$when$ = $(gdelay)$ gdelay refers to the retention delay period when the data should not be retained after the user has unregistered from the service.

Therefore, if $gdelay = gd$, the user's preference is to have personal data retained within the global delay period even after the user unregisters from the service. Retention Obligation for Data Retention*:*

$$Do\ \boldsymbol{ActionDataRetention}\ (\boldsymbol{typeset}, \boldsymbol{fromwhere}, \boldsymbol{time2}, [\boldsymbol{time1}, \boldsymbol{time1} + \boldsymbol{gd}])\ When\ \boldsymbol{TriggerUnregister}(\boldsymbol{typeset}, \boldsymbol{time1})$$

6.7.5 User Preference $\boldsymbol{Rfw}$

User preference Rfw = $(cons, fwpurp, 3rdparty, notify\ )$.

6.7.5.1 Preference of User for Consent: $\boldsymbol{cons}$ = Y => Match with the Obligation

There is an expectation of the following obligation from the service provider side to obtain consent before sharing or transferring personal data to another service provider*:*

$$Do\ \boldsymbol{ActionCollectConsent}(\boldsymbol{typeset}, \boldsymbol{time} - \boldsymbol{tvalue})\ when\ \boldsymbol{TriggerForwardingPersonalData}(\boldsymbol{typeset}, \boldsymbol{time})$$

Inconsistency can occur when a service provider does not receive a corresponding cons = N. This means that no consent has been provided for data collection in the following obligation: Forwarding obligation for consent:

$$Do\ \boldsymbol{ActionCollectConsent}(\boldsymbol{typeset}, \boldsymbol{time} - \boldsymbol{tvalue})\ when\ \boldsymbol{TriggerForwardPersonalData}(\boldsymbol{typeset}, \boldsymbol{time})$$

6.7.5.2 Preference of User for Personal Data Forwarding Purpose $\boldsymbol{fwpurp}$

The user preference for forwarding requires the service provider to have an obligation to conduct personal data transfer whenever there is a request for personal data forwarding. Forwarding obligation for $purpose$:

$$When\ \boldsymbol{TriggerForwardPersonalData}(\boldsymbol{typeset}, \boldsymbol{purposes}), then$$
$$\boldsymbol{SubsetOf}\ (\boldsymbol{purposes}, \boldsymbol{fwpurp})$$

6.7.5.3 Preference of User for Third-party Forwarding Purpose $\boldsymbol{3rdparty}$

The user preference for third-party forwarding of personal data creates an obligation to list who the third-party recipient is of the user's personal data for verification and audit purposes. Forwarding obligation for $3rdParty$ forwarding:

$$When\ \boldsymbol{TriggerForwardPersonalData}(\boldsymbol{typeset}, \boldsymbol{3rdParty}\ ), then$$
$$\boldsymbol{SubsetOf}\ (\boldsymbol{purposes}, \boldsymbol{fwpurp}, \boldsymbol{3rdParty})$$

6.7.5.4 Preference of User for Third-party Forwarding Notification $\boldsymbol{notify}$

This user forwarding preference means that the user expects the service provider to send a notification to the user if the user's personal data are about to be forwarded to another service provider. Forwarding obligation for notification:

$$Do\ \boldsymbol{ActionForwardingNotification}(\boldsymbol{typeset}, \boldsymbol{time} - \boldsymbol{tvalue})\ when$$
$$\boldsymbol{TriggerForwardingPersonalData}(\boldsymbol{typeset}, \boldsymbol{time}$$

6.7.6 Compliance Check Syntax Evaluation

To match the SaaS service provider's privacy policy with the data subject's preferences, the SaaS-PPL engine will match based on the rule that a SaaS service provider policy is less (or equally as) permissive than the data subject's security and privacy preferences, as captured in the NDPR, was followed.

For example, in the collection phase, both service provider policy (Pol) and customer requirements (REQ) were matched to show how compliance can be achieved using the properties expressed below.

6.7.6.1 Property 1

$(Pol \leq REQ)$ if (for every $Pol\_typeset\_1$ in Pol there is a $R\_typeset\_1'$ *in* REQ *such that* $Pol\_typeset\_1 \leq R\_typeset\_1$)

Property 1 means the service provider complies with the privacy and data protection regulations when every service provider policy typeset is less than or equal to the user preferences If and only if there are corresponding, or matching typesets in the user preference typesets.

6.7.6.1 Property 2

$$Pol\_typeset\_1 \leq R\_typeset\_1' \, iff \; typeset\_1' \subseteq typeset\_1, and \; Pcol \leq Rcol, Pproc \leq Rproc, \ldots, Pret \leq Rret$$

Property 2 means the service policy is in compliance with the privacy and data protection regulations when Pol_typset is less than or equal to the user preferences R_typset and if, and only if, the typeset is a subset of the user preferences subsets and the data collection $Pcol$ is less than or equal to the user preferences in the $Rcol$ subsets.

6.7.6.2 Property 3

$Pcol \leq Rcol \, iff \; (Pcol.cons = N \,\&\, Rcol.cons = N)$ or $Pcol.cons = Y, and \; Rcol.cons \; can \; be \; N \; or \; Y$, and $(Pcol.cpurp \subseteq Rcol.cpurp)$

The data collection obligation properties of the sub-policy $Pcol$ are less than or equal to the user preferences for data collection $Rcol$ if and only if the input sub-policy element $Pcol.cons$ is equal to No and the user preference element $Rcol.cons$ is equal No – otherwise, where the service provider sub-element for consent $Pcol.cons$ is equal to Y and the corresponding user preference is either N or Y, and the service provider sub-policy element $Pcol.cpurp$ typeset is a subset of user preferences subsets of $Rcol.cpurp.$

6.7.6.3 Property 4

$$Pproc \leq Rproc\ iff\ (Pproc.cons = N \,\&\, Rproc.cons = N)\ or\ Pproc.cons = Y \text{ and } Rproc.cons\ can\ be\ N\ or\ Y, \text{ and } (Pproc.procpurp \subseteq Rproc.procpurp)\ (Pproc.whocanproc \subseteq Rproc.whocanproc)\ (Pproc.notify \subseteq Rproc.notify)$$

The data processing obligation properties of the sub-policy $Pproc$ are less than or equal to the user preferences for data processing $Rproc$ if and only if the input sub-policy element $Pproc.cons$ and the user preference element $Rproc.cons$ are equal to N – otherwise, where the service provider sub-element for processing $Pproc.cons$ is equal to Y and the corresponding user preference is either N or Y, and the service provider sub-policy elements $Pproc.procpurp, Pproc.whocanproc$, and $Pproc.notify$ typesets are subsets of the user preferences subsets of $Pproc.procpurp, Pproc.whocanproc,$ and $Pproc.notify$.

6.7.6.4 Property 5

$Pstr \leq Rstr\ iff\ (Pstr.wherestore = N \,\&\, Rstr.wherestore = N)$ or $Pstr.wherestore = Y\ and\ Rstr.wherestore\ can\ be\ N\ or\ Y,$ and $(Pstr.howstore \subseteq Rstr.howstore)\ (Pstr.notify \subseteq Rstr.notify)$

The service provider policy obligations for storage sub-policy $Pstr$ are less than or equal to the user preferences for data storage $Rstr$ if the input sub-policy element $Pstr.wherestore$ is equal to No and $Rstr.wherestore$ are equal to N – otherwise, where $Pstr.wherestore$ is equal to a Yes and the user preferences for $Rstr.wherestore$ is Yes for each data storage location, and where the service provider sub-policy elements for $Pstr.howstore$ are a subset of the user preferences subset of $Rstr$. howstore, then $Pstr.notify$ is a subset of the user preferences in $Rstr.notify$.

6.7.6.5 Property 6

$$Pret \leq Rret\ iff\ (Pret.placeret = N \,\&\, Rret.placeret = N) \text{ or } Pret.placeret = Y\ and\ Rret.placeret\ can\ be\ N\ or\ Y, \text{ and } (Pret.rdelay \subseteq Rret.rdelay)\ (Pret.geld \subseteq ret.geld)\ (Pret.notify \subseteq Pret.notify)$$

The service provider policy obligations for the data retention sub-policy is compliant when $Pret$ is less than or equal to the user preferences for data retention $Rret$ if and only if the input sub-policy element $Pret.placeret$ and $Rret.placeret$ are equal to N – otherwise, where $Pret.placeret$ is equal to Y and the user preferences for $Rret.placeret$ are Y, and retention policy elements on delay are compliant when service provider policy elements $Pret.rdelay$, $Pret.geld$, and $Pret.notify$ are subsets of the user delay preferences $Rret.rdelay, Pret.geld,$ and $Pret.notify.$

6.7.6.6 Property 7

$$Pfw \leq Rfw\ iff\ (Pfw.cons = N \,\&\, Rfw.cons = N) \text{ or } Pfw.cons = Y\ and\ Rfw.cons\ can\ be\ N\ or\ Y, \text{ and } (Pfw.fwpurp \subseteq Rfw.fwpurp)\ (Pfw.3rdparty \subseteq Rfw.3rdparty)\ (Pfw.notify \subseteq Rfw.notify)$$

On data forwarding, the service provider is compliant when the service provider data forwarding policy Pfw is less than or equal to the user data forwarding preferences of the user Rfw. The service provider is also compliant with the data protection regulation if and only if the sub-policy element for consent $Pfw.cons$ and $Rfw.cons$ are equal to N – or when $Pfw.cons$ and $Rfw.cons$ are equal to Y. Additionally, the service provider sub-policy for forwarding purpose $Pfw.fwpurp$ is a subset of the user preferences for forwarding $fwpurp,$ and the list of recipients $Pfw.3rdparty$ is a subset of $Rfw.3rdparty.$

6.8 Chapter Summary

In this chapter, the research question (RQ3) on how privacy and data protection requirements are achieved by presenting the SaaS-PPL specification language alongside PPL evaluation. SaaS-PPL extended the logic, syntax, and semantics for reasoning about security, privacy, and data protection. Thus, achieving the research objective three (3). The language's logic is motivated by the principles of PbD and the end-to-end concept of the data life cycle (Vinh, 2018)]. The syntax is based on PPL syntax, where an obligation is expressed using the Trigger–Action pair.

Service providers and user preferences were defined, as were the sub-policies for each of the stages of the data life cycle and the semantics for each of the policies. Last, detailed user preference obligations and triggers were provided for each sub-policy element based on the extended PPL structure and semi-formal methods and logic. This systematic development of the language helped avoid the ambiguous semantics that has plagued other privacy languages.

CHAPTER SEVEN

7.0 Case Study: Smart Petrol Station SaaS Application

In this chapter, the researcher illustrates the semi-formal specifications and concepts mentioned in Chapter 6 using a smart petrol station scenario powered by a SaaS retail application. Based on this semi-formal illustration, several concrete design recommendations are made to the proposed system developers. Specifically, consent and collection purpose notifications, in compliance with the NDPR, should be implemented to allow data subjects to exercise their rights.

7.1 Overview

The Smart point of sale (POS) pay-at-the-pump petrol station platform is an innovative SaaS solution aiming to provide unique services and time-saving experiences for customers. Customers request services and receive feedback from the interactive system. However, the NDPR forbids data collection and data processing from customers without a mechanism for consent and authentication that complies with the NDPR. Figure 40 depicts interactions between different actors in a system that deals with customer requests in an NDPR-compliant manner.

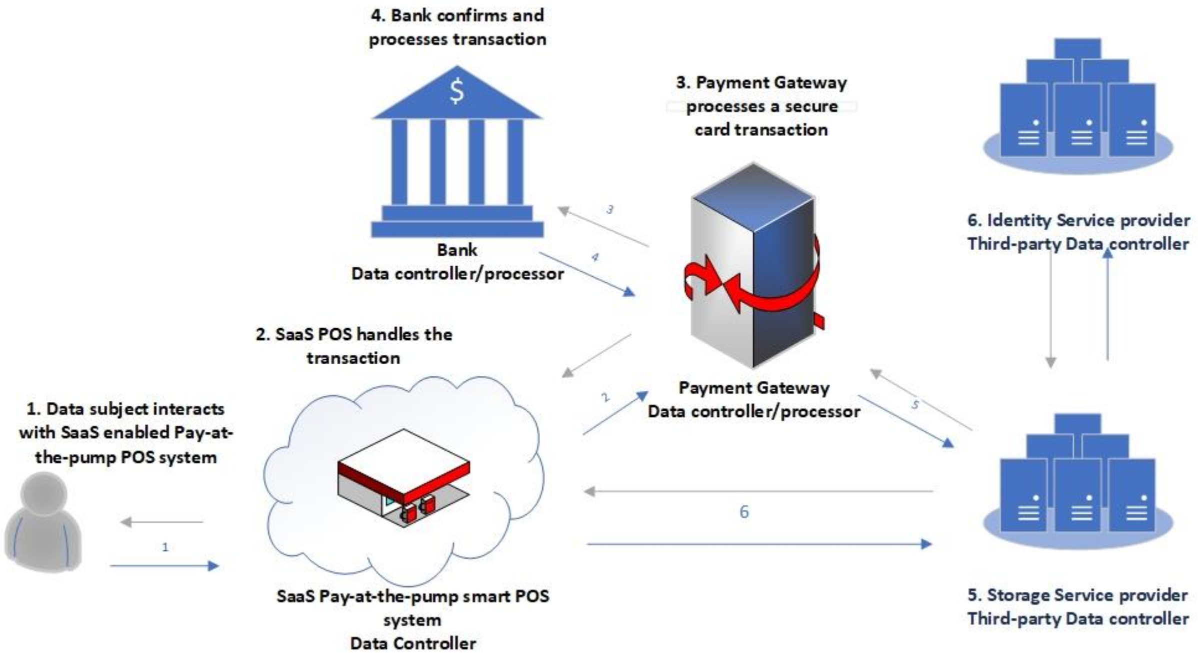

4. Bank confirms and processes transaction
$
Bank
Data controller/processor
3. Payment Gateway processes a secure card transaction
Payment Gateway
Data controller/processor
6. Identity Service provider
Third-party Data controller
2. SaaS POS handles the transaction
1. Data subject interacts with SaaS enabled Pay-at-the-pump POS system
SaaS Pay-at-the-pump smart POS system
Data Controller
5. Storage Service provider
Third-party Data controller
1
2
3
4
5
6

Figure 40: Pay-at-the-pump POS system

1. The user enters their personal data, such as their name, address, and payment information to pay for services using the SaaS pay-at-the-pump POS system.
2. The SaaS pay-at-the-pump service provider collects, processes, retains, stores, and shares the user’s data with other service providers such as identity, payment service, banking, and storage service providers who do not have any data handling obligations to the user or data subject.
3. The payment gateway processes the personal data and payment information in conjunction with the identity and banking service provider.
4. The banking service provider responds with an approval or denial of request message, depending on the account balance.

5. On behalf of the service provider, the storage service provider stores the personal data and transaction history in the transaction chain.
6. SaaS pay-at-the-pump POS system service provider share and store personal data on the storage service provider’s infrastructure.

In the smart petrol station scenario above, customers or data subjects interacts online with the smart SaaS-enabled pay-at-the-pump POS system to pay for fuel and other services.

The SaaS application enables the use of petrol station services using a pay-at-the-pump POS system to serve two utility goals: allowing a customer to pay for products and allowing them to receive notifications about the transaction's completion from the POS SaaS application platform. All interactions with the SaaS application are directed towards the service provider, the third-party payment platform, and the storage service provider.

The POS platform reduces the number of challenges the customer faces in service delivery. The customer is the data subject in this context. However, third-party service providers, such as the payment gateway and the storage company, can obtain the data subject’s sensitive and personal data from the SaaS application platform's transaction information. They have no direct obligations of privacy and data protection to the data subject or customer. More security- and privacy-focused POS SaaS application solution can rely on SaaS-PPL to deliver transaction information to the customer, the SaaS application service provider, and any other third-party service providers in a way that enforces the principles of the NDPR and ensures data privacy and protection.

However, the POS SaaS application relies on third-party services for computing, storage, and other services, making it difficult for the service provider to ensure compliance with data protection regulations, such as the NDPR, in transactions such as in this scenario.

This research proposes a privacy policy language approach for the specification of properties of data protection regulations. SaaS-PPL intends to specify these properties at a granular level to enable the platform to ensure privacy from the data collection stage and regulate how data are shared with third parties across the entire transaction cycle. The diagram below depicts how personal data flow in the platform, including how the obligation engine matches the service provider and user preferences.

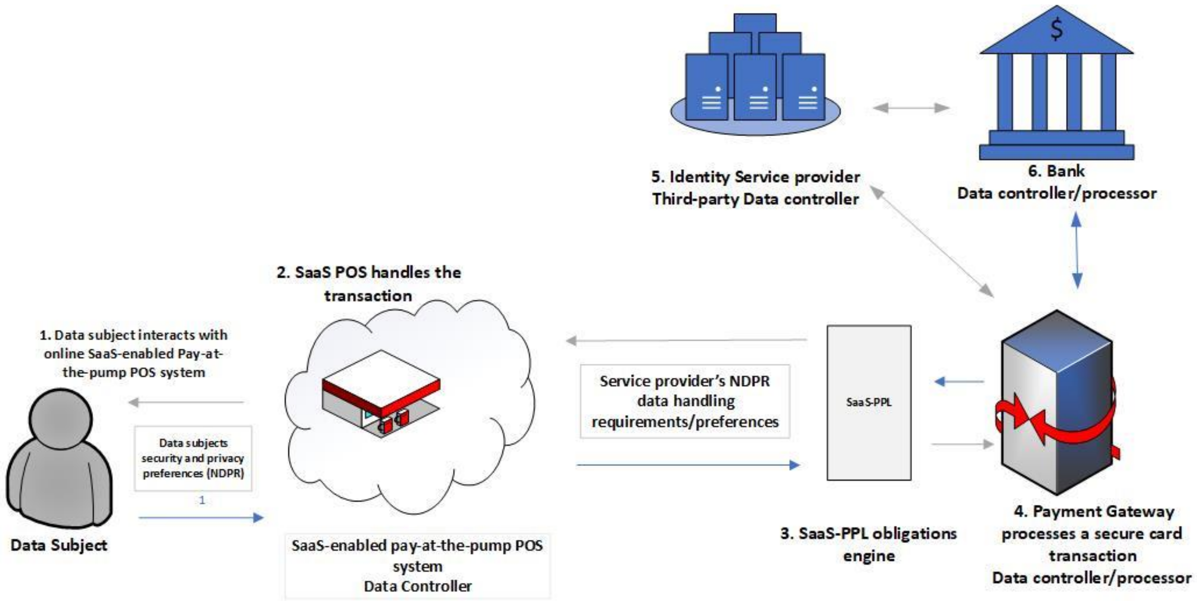

5. Identity Service provider
Third-party Data controller
6. Bank
Data controller/processor
2. SaaS POS handles the transaction
1. Data subject interacts with online SaaS-enabled Pay-at-the-pump POS system
Data subjects security and privacy preferences (NDPR)
1
Data Subject
Service provider's NDPR data handling requirements/preferences
SaaS-PPL
SaaS-enabled pay-at-the-pump POS system
Data Controller
3. SaaS-PPL obligations engine
4. Payment Gateway processes a secure card transaction
Data controller/processor

Figure 41: Pay-at-the-pump POS system SaaS-PPL enabled

7.2 Roles, Responsibilities, and Properties

SaaS-PPL identifies different roles for actors, as identified in the PPL and data protection regulations such as *data subject*, the *data controller*, and *third-party data controller*, and properties such as

$$cons, cpurp, procpurp, whocanuse, notify$$

There are two relations between the properties enabling compliance by matching service provider preferences and user preferences at each data life cycle level.

Table 9: SaaS-PPL actors

Role	Responsibility	Properties
Data subject	Is responsible for providing consent and personal data, such as registration and payment information data	$cons$ ▪ $Do\ ActionCollectConsent\ (typeset, time - tvalue)\ when\ TriggerCollectPersonalData\ (typeset, time)$
Data controller	Is responsible for clarifying the purpose of collection and processing, identifying who is allowed to use the data, and notifying the data subject	$cpurp, procpurp\ whocanuse\ notify$ ▪ $Do\ ActionProcessConsent\ (typeset, time - tvalue) when\ TriggerProcessData\ (typeset, time)$
Data controller	Is responsible for providing the location of the encrypted storage service	$wherestore$ $Do\ ActionSaveEncryptedData\ (typeset, spkey, SpOwnServer, time$ $when\ TriggerStoreData\ (typeset, time)$

7.3 Evaluation and NDPR Compliance Consideration/Basis

The salient goal of the proposed pay-at-the-pump POS system is to achieve compliance with the NDPR. Many of the requirements of the NDPR have been expressed in the logic. For simplicity, five specific requirements for the collection, usage, storage, retention, and forwarding of data that can be met – and even then only when the data subject's preferences (see Section 6.7) match the data controller's obligations (see the NDPR's requirements in Section 5.1.4) – are listed below.

7.3.1 Privacy and Utility

There are two utility goals of SaaS-PPL-enabled pay-at-the-pump POS. First, customers should be able to pay for services and receive feedback in the form of a notification at the end of the service fulfilment without any violation of their data's security and privacy. Incorporating SaaS-PPL can help achieve this utility goal and promote privacy and data security goals. The second utility goal is data protection regulation compliance.

7.4 Evaluation Examples

- **Data Collection:** To serve the customer at the smart petrol station, the customer's personal and payment data should be collected using a SaaS retail application. To fulfil service requests such as refuelling and car servicing, the following values are expressed:

$$Pcol = (cons, cpurp)\ (cons\ = Y, cpurp$$
$$= \{payment, registration, buyPetrol, buySnacks\}).$$

According to Section 2.3 of the NDPR,

- *No data shall be obtained without making the specific purpose of collection known to the data subject.*
- *The data controller is under the obligation to ensure that consent of the data subject has been obtained without fraud, coercion, or undue influence.*

- **Processing:** At this stage, the service provider of the retail SaaS application processes the customer's personal data to serve the data subject (i.e. the customer). In this case, the following values are expressed:

$Pproc = (cons, procpurp, whocanuse, notify)\ (cons\ = Y, procpurp$
$= \{payment, registration, buygas, \}\ whocanuse$
$=\ \{authorized\ personnel, authorized\ third$
$- party, authorized\ identity\ service\ provider\}, \{notify$
$=\ Y\ via\ email\ or\ SMS\ to\ confirm\ data\ processing\})$

According to Part 2*, Section 2.2 (subsections (a–e)) of the NDPR, the service provider must have a* ***<u>lawful basis</u>*** *and obtain the data subject's consent before* ***<u>processing</u>*** *personal data.*

- **Storage:** At this stage, the personal data are stored to serve the data subject based on the subject's data handling preferences. The SaaS service provider can store the data on third-party storage infrastructure depending on the data storage and processing purpose. In this case, the following values are expressed:

$$Pstr = (wherestore, howstore, notify), where\ decl\{Y, N\}\ (Wherestore = \{SPstorage, 3rdPartyStorage\}$$

$Howstore$ = {Available meaning, data are accessible to the service provider, hidden meaning data are encrypted and inaccessible to the service provider}, {notify = Y via email, SMS, point of sale to confirm and accept data storage request})

According to Part 2, Section 7 (subsection (h)) and Section 12 of the NDPR, organisations are required to enforce data protection when they collect, ***store,*** *or* ***process*** *data only for the required* ***purposes*** *for which they are collected and stored.*

- **Retention:** Relying on consent and lawful purposes for retention as required by the NDPR, the SaaS service provider and their third-party partners retain or destroy personal data to maintain compliance. In this case, the following values are expressed:

$$Pret = (placeret, when, notify), where\ notify\ \in\ \{Y, N\},)\ Placeret = \{mainstorage, backupstorage, 3rdPartyStorage\}, When = (\{rdelay, gd\ numerical\ retention\ delay\ value\}, notify = Y\ \{email, SMS, POS\ to\ confirm\ data\ retention\ policy\ preferences\})$$

In Section 7 and subsection (h) of the NDPR, the data subject's right to be ***forgotten****, to* ***erasure, and to retention or deletion*** *is stated. The data subject shall have the right to ask the controller the erasure or delete their personal data without undue delay, and the controller shall be obligated to comply.*

- **Data Forwarding:** At this stage, the SaaS service provider, as the data controller, is responsible for the personal data that will be collected to enable interactions and services. Data forwarding obligations are matched with the preferences and consent of the owner, giving the following values:

$$\begin{aligned}
&Pfw = (cons, fwpurp, 3rdparty, notify, decl), where\ decl \in \{Y, N\}, cons\\
&= \{Y, N\}, (cons\ = \{Y\}, fwpurp\\
&= \{verifyIdentity, collectPayment, \}\ 3rdParty\\
&= \{ListDataProcessors, identityProvider, paymentGateways\}\ notify\\
&= \ Y\ \{\ email, SMS, POS\ to\ confirm\ data\ forwarding\ policy\ preferences\}\ decl\\
&= \{Y\})
\end{aligned}$$

In Section 7 (subsection (e)) of the NDPR, it is stated that any transfer of personal data that are undergoing processing or are intended for processing after transfer to a third country or an international organisation shall take place only if the data are subject to the rights of the data subject, such as the right to know the legitimate interests of the third party, the right to know the recipients or the category of the recipients, and the right to know about the existence or absence of an adequate decision by NITDA, when the transfer is to a third country or international organisation.

These compliance requirements were expressed and specified for the use case of the NDPR by relying on abstract extension properties to check for a match or a mismatch and by relying on the data subject's obligations/preferences and data controller's obligations/preferences using a matching policy (see Section 7.0)

7.5 Example 2: Data Processing Social Media Data Profiling Scenario

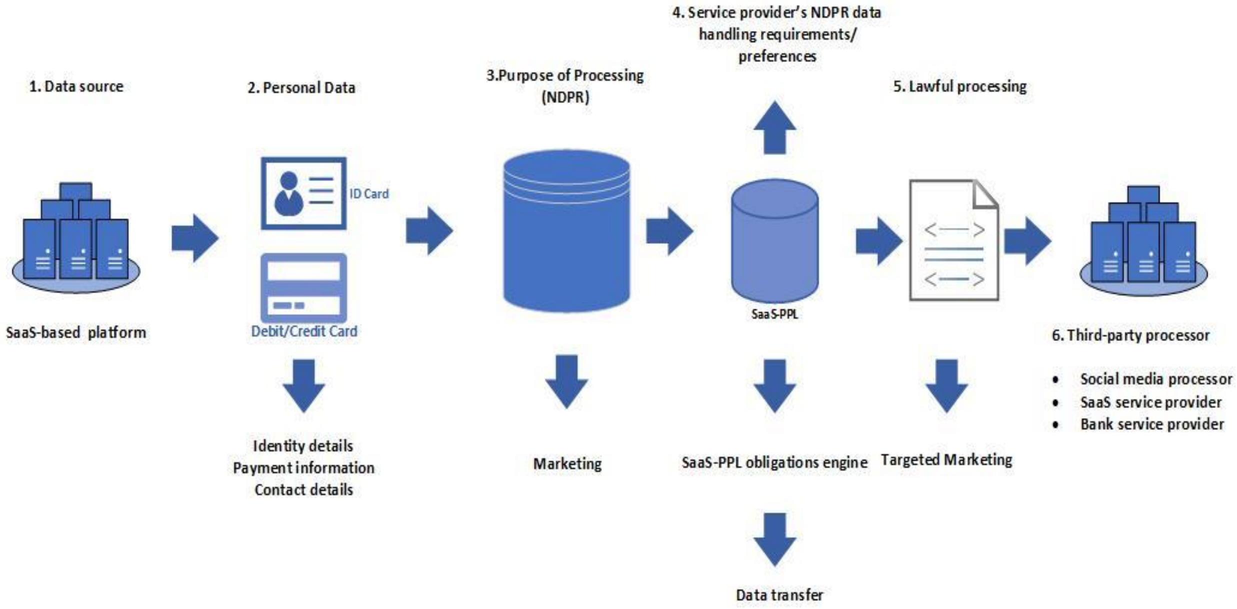


Figure 42: Data Processing Social Media Data Profiling Scenario

7.5.1 Overview

The ability to detect and collect user or customer personal and financial data, preferences, usage behaviours help service providers to discover new ways and prospects with comparable preferences and characteristics when they process and analyse social data (Bello, et al. 2016). Social data is the data that social media users publicly disclose, such as location, language, personal data, and shared links. Marketers use social data to get insight into their customers, leading to more sales or votes (Aggarwal 2011). Social data includes tweets from Twitter, Facebook posts, Pinterest pins, Tumblr postings, and Foursquare and Yelp check-ins (Manovich 2011). For example, Facebook for Business and Twitter Advertisements allow marketers to target individuals likely to respond to their ads.

Social media users willingly make most of their data public, giving businesses easy access. If a ticketing SaaS provider observes that a customer travels a route often, it may target advertisements to encourage them to purchase cheaper tickets.

For example, if someone has posted that they are looking for a new phone, an organisation or business may show them relevant advertisements based on their previous postings in a scenario where data is shared between the social media platform and the SaaS platform.

The first step in developing a customer or user profile is gathering as much data as possible from the social media platform, such as socio-demographic and sales data from current customers who have bought services or goods from the organisation via social media profiling to enhance the effectiveness and accuracy of the organisation their marketing efforts and strategies.

1. Data Source- SaaS application or Platform

In the above example, organisations directly collect personal and financial usage, cookies and preferences data from the users' browser to service the user from the SaaS application or platform, thus serving as the data source.

2. Collection – Personal data

After collecting consent to collect the data, the organisation must satisfy relevant data protection regulation requirements and provide information relating to the lawful purpose of collecting personal data.

3. Purpose of processing - Marketing

The purpose of processing the collected data, including personal data, is for the organisation to target advertisement efforts to the most likely to buy or subscribe to their services. Additionally, the organisations can best determine the effective ways of advertisement by using the data to narrow down the targeted audience by language, age, location, and even gender. Another purpose may be to help the organisation to engage with its existing customers.

4. SaaS-PPL engine

The SaaS-PPL engine in this scenario is applied to ensure that the service provider obligations are matched with the user preferences based on the NDPR data protection regulation.

5. Lawful processing

Here, the SaaS-PPL engine checks that the data collected from the social media platform has a lawful basis of the processing for marketing purposes and that consent has been collected before processing and in line with the provisions of the NDPR.

6. Third-party processor

Finally, within the scenario above, third-party processors process the data for marketing purposes after the SaaS-PPL has established that the data source, consent, purpose, and lawful basis have been satisfied to be processed or used in marketing.

7.6 Chapter Summary

In this chapter, a case study was presented using a SaaS-application-enabled petrol station scenario to demonstrate the approach's feasibility and validate SaaS-PPL. Furthermore, examples of collected data types were provided at each level of the data life cycle with concrete values. Similarly, an evaluation of SaaS-PPL was conducted for privacy, security, and data protection scenarios. However, more work needs to be done to enrich and implement the language and its sub-policies in a real-life SaaS application context, such as a customer relationship management (CRM) or Microsoft Office implementation context.

CHAPTER EIGHT

8.0 Conclusion

8.1 Summary of Thesis

Security, privacy, and regulatory data protection compliance are important concerns to organisations and individuals today. Regulatory compliance expectations are complex and challenging for modern enterprises and individuals alike to understand and manage. Thus, there is a strong need for a generic, semi-formal policy language for classifying text-based privacy and data protection policies and legal requirements into specific sub-policies at each level of the data life cycle. These sub-policies can then be applied to organisations' IT systems and infrastructures, such as SaaS applications.

In this chapter, the researcher summarises the previous chapters and puts the study's contributions into perspective. The chapter also highlights the inherent limitations of the thesis and discusses grounds for future research.

Chapter one provided a general overview of the thesis. The chapter highlighted the research context: the security, privacy, and safety of personal data and challenges SaaS applications face in complying with data protection regulations. The chapter also discussed the research challenges and motivation, formulated the research questions and objectives, outlined the research contributions, and presented an overview of the research methods. Finally, the chapter presented a summary of the thesis as a whole.

Chapter two presented a comprehensive literature review of the fundamentals of SaaS applications; the concepts of privacy, personal data, and privacy by design; and approaches to and challenges of implementing privacy by design. Furthermore, the chapter established a link between SaaS applications, security, privacy, and data privacy.

Additionally, the chapter discussed data protection and data regulations relevant to the research, such as the NDPR (2019) and GDPR (2018). Finally, the chapter discussed security, privacy, and data protection issues in SaaS applications in detail and listed existing approaches to achieving compliance, such as

- Manual internal audits
- Third-party auditing services
- SLAs
- Privacy policy languages

A narrative summary of each of the approaches was presented through the lenses of SaaS applications, security, privacy, and data protection.

Chapter three presented the chosen methodology, provided the rationale for choosing the methodology, and described the research methods. The collection methods used to gather requirements for the SaaS-PPL and answer the research questions were presented.

Further, the chapter presented the principles of design science methods such as the following:

- Design as an artefact
- Problem significance or relevance
- Design evaluation
- Research contributions
- Rigour of the research
- Design as a search process
- Communication of the research.

Similarly, the chapter presented semi-formal methods used to design a semi-formal policy language for the specification of compliance properties in SaaS business applications (referred to as the ‘artefact’). A combination of design science and semi-formal methods was applied to the context of the NDPR using the example of a petrol station scenario.

The chapter also presented semi-formal mathematical proofs to evaluate the formalised artefact’s properties. The evaluation’s objective was to determine whether the design process developed in this study was successful in specifying and matching the privacy and data protection compliance properties of the service provider and users' preferences within the context of NDPR-compliant SaaS applications.

Chapter four presented the principles of the NDPR (2019) and compared the NDPR with the GDPR. The scopes of the two regulations and their personal, material, territorial scopes, and the applicability of the NDPR were discussed.

Definitions of key terms of the NDPR, such as rights, enforcement mechanisms, civil remedies, data subjects, data controllers, and processors, were provided and the possible executions of third-party data transfers were discussed. Similarly, other concepts, such as the data life cycle and the mapping of the compliance requirements and properties, were presented.

Chapter five presented the results of the data collection and analysed them. Furthermore, the chapter provided data visualisations and themes that emerged from the questionnaires and focus group session. These findings and themes were used to understand the concerns expressed by respondents.

Chapter six presented the SaaS-PPL specification language and evaluated PPL. Further, SaaS-PPL extensions, including their logic, syntax, semantics for reasoning and specifying security, privacy, and data protection, were discussed. The logic is motivated by the end-to-end concept of the data life cycle (Butin, Métayer 2015). The syntax is based on the PPL syntax, where an obligation is expressed using the Trigger–Action pair.

Additionally, service providers and user preferences were defined alongside sub-policies for each stage of the data life cycle. Each policy's semantics were defined and the detailed user preferences for each obligation and trigger considered. These were expressed for each of the elements of the sub-policies based on an extended PPL structure, semi-formal methods and logic.

Lastly, to match the SaaS service provider's privacy policy preferences with the data subject's preferences, a semi-formal proof procedure and logic was used based on the rule in the NDPR that a SaaS service provider policy is less (or equally as) permissive than the data subject's preferences.

Chapter seven presented a case study using a SaaS-application-enabled petrol station scenario to demonstrate the SaaS-PPL approach's feasibility and validate SaaS-PPL as a language. Furthermore, the privacy language was evaluated by using it to express the security, privacy, and data protection provisions of the NDPR. The researcher was able to express the main security, privacy, and data protection provisions of the NDPR and show that the regulation exercises all features of SaaS-PPL. Additionally, the language applies to regulations such as the GDPR because it consists of primarily similar provisions regarding permitted communications and forbidden communications. The different contexts of these requirements are captured accurately in SaaS-PPL logic.

The semi-formalised provisions of the NDPR in Section 6.6 through 6.7.6 are useful for evaluating the expressiveness of the logic of privacy, utility, and data protection and all of the stages of the data life cycle. However, they are limited to the data life cycle stages to enforce compliance with the NDPR and because achieving complete formalisation of the security, privacy, and data protection provisions of the regulation is a significant undertaking. Therefore, the researcher focused on specific provisions relating to the data life cycle that were relevant to the research context.

Furthermore, the chapter provided examples of data types collected at each level of the data life cycle with concrete values. Finally, an SaaS-PPL evaluation was conducted using privacy, security, and data protection scenarios to validate the language.

8.2 Overview of Thesis Contributions

Here, the researcher highlights the significance of the thesis contributions in the context of the existing body of knowledge.

The first contribution is a SaaS model focused research and NDPR compliance approach with particular emphasis on achieving privacy, security by complying with data protection regulations such as the NDPR in the areas of privacy of data, security, location, multi-tenancy, usage, storage and data forwarding within the context of SaaS applications. The focus on SaaS applications resulted in new knowledge that may be used as an initial benchmark for policy language extensions. That should be considered when proposing extensions for implementing the language in different scenarios, such as in an On-premises SaaS scenario.

The second contribution is mapping the security and privacy provisions of the NDPR and aligning them to the data life cycle for ease of encoding and specification. SaaS application service providers collect users’ data to offer their applications or services, thus creating the need for organisations to ensure compliance with data handling regulations. This research considers a scenario in which data are collected and transferred from the data subjects to the service provider’s infrastructure. However, this contribution creates a new perspective; the data’s handling could conflict with the data subject’s data handling preferences, raising privacy and data protection concerns (Alkhater, Walters et al. 2018) over a potential loss of control over personal data (Trapero, Modic et al. 2017).

This was achieved by analysing data controllers’ obligations, as detailed in the NDPR principles, allowing for the specification of policies across data collection stages, usage, storage, deletion and retention, and forwarding.

The third contribution is the condensed conversion of the data protection regulation requirements to apply to SaaS applications and presenting them using a semi-formal policy language. This was done by maintaining the fundamental roles defined in PPL. Syntax was used to specify and express the data protection properties of the NDPR, and the syntax of the policy language was defined and aligned to the data life cycle.

The fourth contribution is using the compliance check syntax to show proof of compliance when all properties are matched and to demonstrate the validity and applicability of SaaS-PPL in the context of SaaS applications. The compliance check syntax was designed to show proof of conformance when a service provider’s preferences are matched with the data subjects’ preferences.

The last contribution stemmed from the survey of policy languages proposed in different contexts. The policy language approach review is a new addition to the security, privacy, and data protection literature. To the best of the researcher’s knowledge, no similar review exists. Furthermore, the survey was presented as a narrative summary, with insights into each approach provided and inadequacies highlighted. Thus, this study contributed to the body of knowledge on privacy security and data protection.

8.3 Thesis Limitations

In this research, the researcher considered the context of SaaS applications and the NDPR regulation within a retail scenario and, therefore, not a generalisation of every scenario or case. Likewise, the specification and encoding only considered the personal data regulatory obligations imposed by the NDPR at every stage of the data life cycle. This practice may differ from the requirements of other technologies and systems with different elements and features.

Furthermore, the study is entirely from the SaaS model perspective. Thus other models such as IaaS and PaaS or even sub-models such as CaaS and FaaS may have different data protection compliance requirements.

Furthermore, the methodology approach of design science and semi-formal method were used at different stages. Therefore, depending on the stage, different limitations of the methods were identified. A significant limitation experienced at the qualitative stage was the collected volume, making analysis and interpretation time-consuming and difficult. Additionally, the researcher found it difficult to avoid being present during the focus group session, affecting their responses.

One significant challenge was ensuring that the translation and encoding of the compliance requirements of the data protection provisions of the NDPR would accurately capture the semantics of the NDPR. The semi-formal methods had several known limitations: (1) the refinement rules were not sufficient to guarantee that a specification would satisfy the user’s fundamental requirements if it satisfied the specification; (2) the existing refinement rules were not always applicable in theory during successive refinements; and (3) the refinement rules were challenging to apply effectively in practice because of various kinds of uncertainties and resource constraints (Shaoying Liu, R. Adams 1995, Serna, Serna 2017).

The extensions of SaaS-PPL were carried out using semi-formal techniques (an approach considered difficult) (Parnas 2010). A more lightweight extension, such as the unified modelling language UML profiling or business process model and notation (BPMN) approach, might have been easier and could have been reused and applied to other contexts (P. Ballarini, M. Batteux et al. 2018).

In the research, consideration was given to evaluating the policy language against privacy, security, and data protection scenarios; while it is challenging to evaluate a privacy language scientifically, evaluating a portion of the logic of security, privacy, and data protection can be carried out by using syntax for checking policy consistency, combining policies, and enforcing compliance. Policy combination, which is problematic in PPL, is formulated easily using logical conjunction and disjunction.

Another significant limitation discovered in the research is the enforcement of the NDPR. While the NDPR is similar to the GDPR, it is very different when it comes to enforcement. The responsibility for enforcing NDPR is embedded within the bureaucracy of the NITDA in Nigeria, which does not have the resources and mechanisms to effectively enforce compliance with the NDPR at the national level thus creating an urgent need for rethinking the NITDA structure the adoption of mechanisms such as the SaaS-PPL into the NITDA enforcement architecture.

To the best of the researchers' knowledge, the approach to compliance with data protection regulations proposed in this research is the most appropriate. It provides a specification language to help organisations express data protection regulation requirements of the NDPR and any other similar requirements. Overall, the proposed approach mainly demonstrated that it is feasible to comply with data protection regulations by employing the privacy policy language approach and expressing the requirements at a higher level of abstraction.

8.4 Future Research Perspectives

In the inevitable big data future, critics and sceptics argue that privacy will have no place. The researcher disagrees with this argument. However, the researcher argues that the concept of privacy properly understood within the perspective of a data driven world, privacy rules will be an essential and valuable part of our digital future, especially if human values on which today’s political, social and economic institutions have been built are retained.

The researcher makes three significant points. Firstly, the thinking around the concept of ‘’privacy’’ is not merely about the right of the individual to be left alone and his data, but the concept of privacy should be perceived as the regulations we employ to regulate how information is collected and used stored, and shared. Therefore, privacy and data protection rules can be understood as rules on how to handle data, and in today’s information age, where societies are built on how they utilise data, regulation of data or information becomes sacrosanct or inevitable.

Secondly, having the right to be left alone as encapsulated in the concept of privacy should not be the only stimulating factor or basis of privacy, but rather human values should be at the core of the quest to enhance the privacy of the individual's data and the society at large. These human values must encompass other areas that overlap with privacy principles, such as trust issues, security, and other issues relating to identity and equality.

Third, the researcher argues that with advancements in the cloud, blockchains, AI, IoT’s, intelligent systems and even central and decentralised platforms, personal data, big data must be kept private and securely in many different ways. Data protection regulations are one way of achieving that through compliance systems and tools. However, the development of new ideas around ethical notions of personal data handling will be highly required.

To that effect, the researcher has already started engaging with the Nigerian government through the NITDA agency and lawmakers on the need to further look at the data protection regulation and restructure it to effectively enforce the privacy and security of personal data.

8.5 Future Research Directions

Furthermore, based on the limitations raised above, a summary of future works providing a basis for either consolidating the outcomes of this thesis or further extending the research's method or approach towards supporting the development of variations of policy languages for SaaS applications scenarios.

The following are some of the directions for future work:

- As the research focused mainly on SaaS and retail context, future research areas may consider the sub-models of the cloud computer such as FaaS, DaaS and CaaS to enforce data protection compliance on social data collected from containerised solutions Container as a Service (CaaS) implementations.
- Future studies may wish to consider another industry or scenario, such as in the banking sector, to investigate and explore compliance efforts in areas such as their processes and how they process personal data.
- Additionally, future studies can develop a cloud-based tool using the theoretical and specification design provided in this thesis and

deploy it as a containerised Docker tool on the Azure platform for compliance checking.

- Future studies can extend the proposed SaaS-PPL to capture cloud models such as PaaS and IaaS to make them more versatile and capable of specifying requirements across all cloud variants of the computing paradigm.
- Future studies can extend and improve the SaaS-PPL in the area of compliance check procedures for matching service provider preferences and data protection requirements, which are usually mapped to user preferences and expectations.
- The research used only a single domain, SaaS applications, and a pay-at-the-pump example to explore the policy language approach to compliance with the NDPR. Further investigation is necessary for other SaaS domains, such as banking, education, and healthcare, to enhance our understanding of the research findings.
- The Nigerian government should consider reviewing the NDPR (2019), taking away the role of enforcement from the NITDA, and establishing the office of information commissioner or a directorate, which will be solely charged with the enforcement of the regulation. There is currently some ambiguity in applying the NITDA regulation, and it is slowing compliance efforts.

  Finally, suppose the Nigerian government wants to be identified as a genuinely interested government and understands the urgent need for security and privacy of personal data in government and private organisations. In that case, policymakers will need to enforce NDPR implementation strictly. Similarly, the government should develop and execute a nationwide data protection awareness programme to highlight citizens' personal data's importance and value. Other developing countries in similar situations may adopt the same suggestion.

8.6 Concluding Thesis Remarks

This thesis has established that approaches to achieving compliance with data protection regulations, including those proposed for implementing policy languages in different contexts, have fallen short of helping achieve compliance with regulations such as the NDPR and GDPR within the context of SaaS applications. Similarly, other compliance approaches, such as manual audits and industry and propriety certifications, have fallen short in security, privacy, data protection compliance, verification, coverage, and scope. Given the established limitations of the existing approaches, this thesis presents a semi-formal SaaS-PPL specification language that can support the specifications of compliance requirements at each granular level of the data life cycle for end-to-end compliance with the NDPR (Schaar, 2010).

References

IEEE Standard for Content Delivery Protocols of Next Generation Service Overlay Network. 2018.

Methodology for deriving a business complexity index through the application of the complexity framework for SaaS. 2015.

A. A. ACHARGUI and A. ZAOUIA, 2016. *Hosted, cloud and SaaS, off-premises ERP systems adoption by Moroccan SMEs: A focus group study.*

A. A. Z. A. IBRAHIM, S. VARRETTE and P. BOUVRY, 2018a. On Verifying and Assuring the Cloud SLA by Evaluating the Performance of SaaS Web Services Across Multi-cloud Providers, *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)* 2018a, pp. 69-70.

A. A. Z. A. IBRAHIM, S. VARRETTE and P. BOUVRY, 2018b. On Verifying and Assuring the Cloud SLA by Evaluating the Performance of SaaS Web Services Across Multi-cloud Providers, *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)* 2018b, pp. 69-70.

A. CAVOUKIAN, 2020. *Understanding How to Implement Privacy by Design, One Step at a Time.*

A. GHORBEL, M. GHORBEL and M. JMAIEL, 2017. PRIARMOR: An IaaS Solution for Low-Level Privacy Enforcement in the Cloud, *2017 IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* 2017, pp. 119-124.

A. JARZEBOWICZ and K. POLOCKA, 2017. Selecting requirements documentation techniques for software projects: A survey study, *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)* 2017, pp. 1189-1198.

A. MANCHAR and A. CHOUHAN, 2017. *Salesforce CRM: A new way of managing customer relationship in cloud environment.*

A. NUGRAHA, S. H. SUPANGKAT and D. NUGROHO, 2012. *Goesmart: Social media education in cloud computing.*

A. Q. ALI, A. B. M. SULTAN, A. A. A. GHANI and H. ZULZALIL, 2019. *A Systematic Mapping Study on the Customization Solutions of Software as a Service Applications.*

A. R. WANI, Q. P. RANA and N. PANDEY, 2017. Cloud security architecture based on user authentication and symmetric key cryptographic techniques, *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* 2017, pp. 529-534.

A. S. AHMADIAN and J. JÜRJENS, 2016. Supporting Model-Based Privacy Analysis by Exploiting Privacy Level Agreements, *- 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)* 2016, pp. 360-365.

A. SHI, Y. XIA and H. ZHAN, 2010. *Applying cloud computing in financial service industry.*

ABUHUSSEIN, A., BEDI, H. and SHIVA, S., 2012. Evaluating security and privacy in cloud computing services: A Stakeholder's perspective, *2012 International Conference for Internet Technology and Secured Transactions*, Dec 2012, pp. 388-395.

ACHARGUI, A. and ZAOUIA, A., 2015. Open Source ERP, what opportunity for Moroccan SMEs? Case study of a Moroccan agribusiness SME. *Journal of African Research in Business & Technology,* .

AGBALI, M., DAHIRU, A.A., OLUFEMI, G.D., KASHIFU, I.A. and VINCENT, O., 2020. Data Privacy and Protection: The Role of Regulation and Implications for Data Controllers in Developing Countries, *International Conference on Social Implications of Computers in Developing Countries* 2020, Springer, pp. 205-216.

AGGARWAL, C.C., 2011. An introduction to social network data analytics. *Social network data analytics.* Springer, pp. 1-15.

ALBRECHT, J.P., 2016. How the GDPR will change the world. *Eur.Data Prot.L.Rev.,* **2**, pp. 287.

ALI, A., WARREN, D. and MATHIASSEN, L., 2017. *Cloud-based business services innovation: A risk management model.*

ALKHATER, N., WALTERS, R. and WILLS, G., 2018. *An empirical study of factors influencing cloud adoption among private sector organisations.*

ALSHAMMARI, M. and SIMPSON, A., 2018. Privacy architectural strategies: an approach for achieving various levels of privacy protection, *Proceedings of the 2018 Workshop on Privacy in the Electronic Society* 2018, pp. 143-154.

ALSHAMMARI, A., ALHAIDARI, S., ALHARBI, A. and ZOHDY, M., 2017. Security Threats and Challenges in Cloud Computing, *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, June 2017, pp. 46-51.

ALTMAN, I., 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.

ALTORBAQ, A., BLIX, F. and SÖRMAN, S., 2017a. Data subject rights in the cloud: A grounded study on data protection assurance in the light of GDPR, *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec 2017a, pp. 305-310.

ALTORBAQ, A., BLIX, F. and SÖRMAN, S., 2017b. Data subject rights in the cloud: A grounded study on data protection assurance in the light of GDPR, *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec 2017b, pp. 305-310.

ALTORBAQ, A., BLIX, F. and SÖRMAN, S., 2017c. Data subject rights in the cloud: A grounded study on data protection assurance in the light of GDPR, *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec 2017c, pp. 305-310.

ALVES-FOSS, J., 1999. *Formal syntax and semantics of Java.* Springer Science & Business Media.

AL-ZABEN, N., ONIK, M.M.H., YANG, J., LEE, N. and KIM, C., 2018. General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management, *2018 International Conference on Computing, Electronics Communications Engineering (iCCECE)*, Aug 2018, pp. 77-82.

ANTONIOU, J. and ANDREOU, A., 2019. Case Study: The Internet of Things and Ethics. *The Orbit Journal,* **2**(2),.

ASHALATHA, R. and AGARKHED, J., 2016. Multi tenancy issues in cloud computing for SaaS environment, *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)* 2016, IEEE, pp. 1-4.

ASUQUO, A., 2019. The Principles of Nigerian Data Protection Law. *Available at SSRN 3408775,* .

AUSTIN, L., 2003. Privacy and the Question of Technology. *Law and Philosophy,* **22**(2), pp. 119-166.

AZRAOUI, M., ELKHIYAOUI, K., \ONEN, M., BERNSMED, K., DE OLIVEIRA, A.S. and SENDOR, J., 2015a. A-PPL: An Accountability Policy Language, J. GARCIA-ALFARO, HERRERA-JOANCOMART{\'I JORDI, E. LUPU, J. POSEGGA, A. ALDINI, RO, F. MARTINELLI and N. SURI, eds. In: *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance* 2015a, Springer International Publishing, pp. 319-326.

AZRAOUI, M., ELKHIYAOUI, K., \ONEN, M., BERNSMED, K., DE OLIVEIRA, A.S. and SENDOR, J., 2015b. A-PPL: An Accountability Policy Language, J. GARCIA-ALFARO, HERRERA-JOANCOMART{\'I JORDI, E. LUPU, J. POSEGGA, A. ALDINI, RO, F. MARTINELLI and N. SURI, eds. In: *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance* 2015b, Springer International Publishing, pp. 319-326.

AZRAOUI, M., ELKHIYAOUI, K., \ONEN, M., BERNSMED, K., DE OLIVEIRA, A.S. and SENDOR, J., 2015c. A-PPL: An Accountability Policy Language, J. GARCIA-ALFARO, HERRERA-JOANCOMART{\'I JORDI, E. LUPU, J. POSEGGA, A. ALDINI, RO, F. MARTINELLI and N. SURI, eds. In: *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance* 2015c, Springer International Publishing, pp. 319-326.

B. LI, Z. LI, Y. TAN and J. YU, 2021. CoFunc: A unified development framework for heterogeneous FaaS computing platforms, - *2021 International Conference on*

Communications, Information System and Computer Engineering (CISCE) 2021, pp. 726-730.

B. SPASIC, A. TH. RATH, P. THIRAN and N. BOUCART, 2018a. *Security Pattern for Cloud SaaS: from system and data security to privacy.*

B. SPASIC, A. TH. RATH, P. THIRAN and N. BOUCART, 2018b. *Security Pattern for Cloud SaaS: from system and data security to privacy.*

BANIROSTAM, H., HEDAYATI, A., ZADEH, A.K. and SHAMSINEZHAD, E., 2013. A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure, *2013 UKSim 15th International Conference on Computer Modelling and Simulation*, April 2013, pp. 717-721.

BARONA, R. and ANITA, E.A.M., 2017. A survey on data breach challenges in cloud computing security: Issues and threats, *2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT)*, April 2017, pp. 1-8.

BAUMGARTEN, A., ISHERWOOD, R. and ROESNER, S., 2014. *Microsoft System Center 2012 R2 Compliance Management Cookbook.* Packt Publishing Ltd.

BEDNAR, K., SPIEKERMANN, S. and LANGHEINRICH, M., 2019. Engineering Privacy by Design: Are engineers ready to live up to the challenge? *The Information Society,* **35**(3), pp. 122-142.

BELLO-ORGAZ, G., JUNG, J.J. and CAMACHO, D., 2016. Social big data: Recent achievements and new challenges. *Information Fusion,* **28**, pp. 45-59.

BENGHABRIT, W., GRALL, H., ROYER, J., SELLAMI, M., AZRAOUI, M., ELKHIYAOUI, K., \ONEN, M., SANTANA DE OLIVEIRA, A. and BERNSMED, K., 2014. A Cloud Accountability Policy Representation Framework, *Proceedings of the 4th International Conference on Cloud Computing and Services Science* 2014, SCITEPRESS - Science and Technology Publications, Lda, pp. 489-498.

BERENDT, B., GÜNTHER, O. and SPIEKERMANN, S., 2005. Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM,* **48**(4), pp. 101-106.

BJ\ORNER, D. and HAVELUND, K., 2014. 40 Years of Formal Methods, C. JONES, P. PIHLAJASAARI and J. SUN, eds. In: *FM 2014: Formal Methods* 2014, Springer International Publishing, pp. 42-61.

BJØRNER, D. and HENSON, M.C., 2007. *Logics of specification languages.* Springer Science & Business Media.

BLINK, H., 2020-last update, About Us. Available: https://joinblink.com/.

BREAUX, T. and PEARSON, S., 2016. Ensuring Privacy in Clouds. *Encyclopedia of Cloud Computing,* , pp. 255.

BRODIN, M., 2019a. A Framework for GDPR Compliance for Small-and Medium-Sized Enterprises. *European Journal for Security Research,* **4**(2), pp. 243-264.

BRODIN, M., 2019b. A framework for GDPR compliance for small-and medium-sized enterprises. *European Journal for Security Research,* **4**(2), pp. 243-264.

BROMLEY, E., MIKESELL, L., JONES, F. and KHODYAKOV, D., 2015. From subject to participant: Ethics and the evolving role of community in health research. *American Journal of Public Health,* **105**(5), pp. 900-908.

BRYMAN, A., 2004. Triangulation and measurement. *Retrieved from Department of Social Sciences, Loughborough University, Loughborough, Leicestershire: www.referenceworld.com/sage/socialscience/triangulation.pdf,* .

BURGOON, J.K., PARROTT, R., LE POIRE, B.A., KELLEY, D.L., WALTHER, J.B. and PERRY, D., 1989. Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships,* **6**(2), pp. 131-158.

BUTIN, D. and MÉTAYER, D.L., 2015. A Guide to End-to-End Privacy Accountability, *2015 IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity*, May 2015, pp. 20-25.

C. A. ARDAGNA, S. DE CAPITANI DI VIMERCATI, G. NEVEN, S. PARABOSCHI, F. PREISS, P. SAMARATI and M. VERDICCHIO, 2010. Enabling Privacy-preserving Credential-based Access Control with XACML and SAML, *2010 10th IEEE International Conference on Computer and Information Technology* 2010, pp. 1090-1095.

C. DUMA, A. HERZOG and N. SHAHMEHRI, 2007. Privacy in the Semantic Web: What Policy Languages Have to Offer, *Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07)* 2007, pp. 109-118.

C. SAATCI and E. S. GUNAL, 2019. Preserving Privacy in Personal Data Processing, *- 2019 1st International Informatics and Software Engineering Conference (UBMYK)* 2019, pp. 1-4.

CAMPBELL, S., GREENWOOD, M., PRIOR, S., SHEARER, T., WALKEM, K., YOUNG, S., BYWATERS, D. and WALKER, K., 2020. Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing,* **25**(8), pp. 652-661.

CANDAN, K.S., LI, W.S., PHAN, T. and ZHOU, M., 2009. Frontiers in Information and Software as Services, *2009 IEEE 25th International Conference on Data Engineering*, March 2009, pp. 1761-1768.

CAVOUKIAN, A., 2008. Privacy in the clouds. *Identity in the Information Society,* **1**(1), pp. 89-108.

CAVOUKIAN, A. and CHIBBA, M., 2018. Start with privacy by design in all big data applications. *Guide to big data applications.* Springer, pp. 29-48.

CHEN, D., LI, X., WANG, L., KHAN, S.U., WANG, J., ZENG, K. and CAI, C., 2015. Fast and Scalable Multi-Way Analysis of Massive Neural Data. *IEEE Transactions on Computers,* **64**(3), pp. 707-719.

CHEN, H., 2016. Architecture strategies and data models of Software as a Service: A review, *2016 3rd International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS)*, Aug 2016, pp. 382-385.

CHEN, J., ABEDIN, F., CHAO, K., GODWIN, N., LI, Y. and TSAI, C., 2015. *A hybrid model for cloud providers and consumers to agree on QoS of cloud services.*

CHEN, Y., CHOU, J. and SUN, H., 2008. *A novel mutual authentication scheme based on quadratic residues for RFID systems.*

CHONG, H. and DIAMANTOPOULOS, A., 2020. Integrating advanced technologies to uphold security of payment: Data flow diagram. *Automation in Construction,* **114**, pp. 103158.

CHOUHAN, P.K., YAO, F. and SEZER, S., 2015. Software as a service: Understanding security issues, *2015 Science and Information Conference (SAI)*, July 2015, pp. 162-170.

CHRIS DALE, February, 27 2019, , DLA Piper- Data Protection Laws of the World 2019.

CONFORMING, A.M., 2018. Proposal for a Privacy Impact Assessment Manual Conforming to ISO/IEC 29134: 2017, *Computer Information Systems and Industrial Management: 17th International Conference, CISIM 2018, Olomouc, Czech Republic, September 27-29, 2018, Proceedings* 2018, Springer, pp. 486.

CORTI, L., VAN DEN EYNDEN, V., BISHOP, L. and WOOLLARD, M., 2019. *Managing and sharing research data: a guide to good practice.* Sage.

CRESWELL, J.W., 2003. A framework for design. *Research design: Qualitative, quantitative, and mixed methods approaches,* , pp. 9-11.

CSA, 2017. *Security Guidance Guidance for Critical Areas of Focus of Cloud Computing v4.0.* Cloud Security Alliance.

CULNAN, M.J. and BIES, R.J., 2003. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues,* **59**(2), pp. 323-342.

CURZON, J., ALMEHMADI, A. and EL-KHATIB, K., 2019. A survey of privacy enhancing technologies for smart cities. *Pervasive and Mobile Computing,* **55**, pp. 76-95.

CUSTERS, B., SEARS, A.M., DECHESNE, F., GEORGIEVA, I., TANI, T. and VAN DER HOF, S., 2019. *EU Personal Data Protection in Policy and Practice.* Springer.

D. BUTIN, M. CHICOTE and D. LE MÉTAYER, 2013. Log Design for Accountability, *2013 IEEE Security and Privacy Workshops* 2013, pp. 1-7.

D. I. M. HASNI, A. SARLAN and R. AHMAD, 2020. Collaborative Visualization Framework for Cross-field Working Group: A Qualitative Focus Group Study, *- 2020 International Conference on Computational Intelligence (ICCI)* 2020, pp. 256-260.

D. J. TJIRARE and F. B. SHAVA, 2017. A gap analysis of the ISO/IEC 27000 standard implementation in Namibia, *2017 IST-Africa Week Conference (IST-Africa)* 2017, pp. 1-10.

D. LI, W. ZHANG, S. ZHOU, C. LIU and W. JIN, 2011. Portal-based design for SaaS system presentation layer configurability, *2011 6th International Conference on Computer Science & Education (ICCSE)* 2011, pp. 1327-1330.

D. MANDAL and C. MAZUMDAR, 2018. Automating Information Security Policy Compliance Checking, *2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT)* 2018, pp. 1-4.

D. S. KIM, T. SHIN and J. S. PARK, 2006. *Access Control and Authorization for Security of RFID Multi-Domain Using SAML and XACML.*

DAHLQVIST, F., PATEL, M., RAJKO, A. and SHULMAN, J., 2019. Growing opportunities in the Internet of Things. *McKinsey, July,* .

DE, S.J. and LE MÉTAYER, D., 2016. PRIAM: a privacy risk analysis methodology. *Data privacy management and security assurance.* Springer, pp. 221-229.

DECEW, J.W., 2015. Privacy and its importance with advancing technology. *Ohio NUL Rev.,* **42**, pp. 471.

DENG, M., ZHENG, M. and GUINOTE, A., 2018. When does power trigger approach motivation? Threats and the role of perceived control in the power domain. *Social and Personality Psychology Compass,* **12**(5), pp. e12390.

DI IORIO, C.T., CARINCI, F., ODERKIRK, J., SMITH, D., SIANO, M., DE MARCO, D.A., DE LUSIGNAN, S., HAMALAINEN, P. and BENEDETTI, M.M., 2020. Assessing data protection and governance in health information systems: a novel methodology of Privacy and Ethics Impact and Performance Assessment (PEIPA). *Journal of medical ethics,* .

DINEV, T., 2014. *Why would we care about privacy?,* .

DLA PIPER, 2020-last update, Data Protection. Available: https://www.dlapiperdataprotection.com/.

DRAKE, G., 2017. Navigating the Atlantic: understanding EU data privacy compliance amidst a sea of uncertainty. *S.Cal.L.Rev.,* **91**, pp. 163.

D'SILVA, G.M., THAKARE, S. and BHARADI, V.A., 2016. Real-time processing of IoT events using a Software as a Service (SaaS) architecture with graph database, *2016 International Conference on Computing Communication Control and automation (ICCUBEA)* 2016, IEEE, pp. 1-6.

E. HUANACHIN-YANCCE, R. C. VEGA and D. MAURICIO, 2019. *Enterprise Content Management Model of Services for Development of Computer Career Thesis.*

E. O. DISI and I. A. ZUALKERNAN, 2009. Compliance-Oriented Process Maps and SLA Ontology to Facilitate Six Sigma Define Phase for SLA Compliance Processes, *2009 International Conference on Management and Service Science* 2009, pp. 1-4.

ELSHEKEIL, S.A. and LAOYOOKHONG, S., 2017. *GDPR Privacy by Design,* .

ENISA EUROPE, 2019-last update, Cloud Standards and Security. Available: https://resilience.enisa.europa.eu/cloud-security-and-resilience/Cloudstandards.pdf.

EVERSON, E., 2016. Privacy by design: Taking ctrl of big data. *Clev.St.L.Rev.,* **65**, pp. 27.

FERRARA, P. and SPOTO, F., 2018. Static Analysis for GDPR Compliance. *ITASEC* 2018.

FUJITA, M., HARRIGAN, P., SOUTAR, G.N., ROY, S.K. and ROY, R., 2020. Enhancing member-institution relationships through social media: The role of other-user engagement behavior and similarity perceptions. *Journal of Business Research,* **121**, pp. 642-654.

G. J. SUJA and S. JOSE, 2016. New approach for highly secured I/O transfer with data on timer streaming, *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* 2016, pp. 885-889.

G. LAATIKAINEN and A. OJALA, 2014. SaaS Architecture and Pricing Models, *2014 IEEE International Conference on Services Computing* 2014, pp. 597-604.

G. Y. LEE, K. J. CHA and H. J. KIM, 2019. *Designing the GDPR Compliant Consent Procedure for Personal Information Collection in the IoT Environment.*

GARTNER INC, September, 12, 2018, 2019-last update, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019. Available: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019.

GAWANMEH, A. and ALOMARI, A., 2015. Challenges in formal methods for testing and verification of cloud computing systems. *Scalable Computing: Practice and Experience,* **16**(3), pp. 321-332.

GIULIO, C.D., SPRABERY, R., KAMHOUA, C., KWIAT, K., CAMPBELL, R.H. and BASHIR, M.N., 2017. Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, June 2017, pp. 50-57.

GJERMUNDRØD, H., DIONYSIOU, I. and COSTA, K., 2016. privacyTracker: a privacy-by-design GDPR-compliant framework with verifiable data traceability controls, *International Conference on Web Engineering* 2016, Springer, pp. 3-15.

GODDARD, M., 2017. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research,* **59**(6), pp. 703-705.

H. SONG, P. H. NGUYEN, F. CHAUVEL, J. GLATTETRE and T. SCHJERPEN, 2019. *Customizing Multi-Tenant SaaS by Microservices: A Reference Architecture.*

HALES, T.C., 2008a. Formal proof. *Notices of the AMS,* **55**(11), pp. 1370-1380.

HALES, T.C., 2008b. Formal proof. *Notices of the AMS,* **55**(11), pp. 1370-1380.

HAN, J. and KIM, J., 2017. Design of SaaS OverCloud for 3-tier SaaS compatibility over cloud-based multiple boxes, *Proceedings of the 12th International Conference on Future Internet Technologies* 2017, pp. 1-4.

HENDRADI, P., ABD GHANI, M.K., MAHFUZAH, S., YUDATAMA, U., PRABOWO, N.A. and WIDYANTO, R.A., 2020. Artificial Intelligence Influence In Education 4.0 To Architecture Cloud Based E-Learning System. *International Journal of Artificial Intelligence Research,* **4**(1), pp. 30-38.

HENZE, M., HILLER, J., SCHMERLING, S., ZIEGELDORF, J.H. and WEHRLE, K., 2016. CPPL: Compact Privacy Policy Language, *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society* 2016, ACM, pp. 99-110.

HEVNER, A. and CHATTERJEE, S., 2010a. Design science research in information systems. *Design research in information systems.* Springer, pp. 9-22.

HEVNER, A. and CHATTERJEE, S., 2010b. Design science research in information systems. *Design research in information systems.* Springer, pp. 9-22.

HEYINK, M., 2012. An Introduction to Cloud Computing-Legal Implications for South African Law Firms. *Law Society of South Africa, Pretoria,* .

HUSSEIN, M.K., MOUSA, M.H. and ALQARNI, M.A., 2019. A placement architecture for a container as a service (CaaS) in a cloud environment. *Journal of Cloud Computing,* **8**(1), pp. 1-15.

IKRAM, M.A., 2020. *AI-driven Service Broker for Simple and Composite Cloud SaaS Selection,* .

INDU, I., ANAND, P.M.R. and BHASKAR, V., 2018a. *Identity and access management in cloud environment: Mechanisms and challenges.*

INDU, I., ANAND, P.M.R. and BHASKAR, V., 2018b. *Identity and access management in cloud environment: Mechanisms and challenges.*

INDUSTRY, P.C., *Data Security Standard.Requirements and Security Assessment Procedures.Version 3.2 PCI Security Standards Council (2016),* .

INFORMATION COMMISIONER'S OFFICE, U., 2019, 2019a-last update, Intention to fine British Airways £183.39m under GDPR for data breach. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

INFORMATION COMMISIONER'S OFFICE, U., 2019b-last update, Intention to fine Marriott Internation Inc more than £99 million under GDPR for data breach. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

INFORMATION COMMISIONER'S OFFICE, U., September 2019, 2019c-last update, What is Personal Data. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013. *ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements.* International Organization for Standardization.

ISLAM, S.H. and BISWAS, G.P., 2011. *A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem.*

ISO, March 14, 2019, 2018-last update, ISO 27001, the international information security standard. Available: https://www.itgovernance.co.uk/iso27001.

IZUOGU, C.E., 2021. Conducting Data Protection Impact Assessments for Online Profiling under the NDPR 2019. *Available at SSRN 3868887,* .

J. JING and J. ZHANG, 2010. Research on Open SaaS Software Architecture Based on SOA, *2010 International Symposium on Computational Intelligence and Design* 2010, pp. 144-147.

J. LEWANDOWSKI, A. O. SALAKO and A. GARCIA-PEREZ, 2013. *SaaS Enterprise Resource Planning Systems: Challenges of Their Adoption in SMEs.*

J. MARGULIES, 2015. *Securing Cloud-Based Applications, Part 1.*

J. TANG, 2020. Artificial Intelligence-based E-commerce Platform based on SaaS and Neural Networks, *- 2020 Fourth International Conference on Inventive Systems and Control (ICISC)* 2020, pp. 421-424.

J. TARAZI and V. L. AKRE, 2013. *Enabling e-Collaboration and e-Pedagogy at an academic institution in the UAE.*

JAATUN, M.G., PEARSON, S., GITTLER, F., LEENES, R. and NIEZEN, M., 2016. *Enhancing accountability in the cloud.*

JANSEN, W.A. and GRANCE, T., 2011. Guidelines on security and privacy in public cloud computing.

JASTI, A., SHAH, P., NAGARAJ, R. and PENDSE, R., 2010. Security in multi-tenancy cloud, *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, Oct 2010, pp. 35-41.

JAYASINGHE, U., LEE, G.M. and MACDERMOTT, A., 2018. Trust-Based Data Controller for Personal Information Management, *2018 International Conference on Innovations in Information Technology (IIT)*, Nov 2018, pp. 123-128.

JENNIFER ROWLEY, 2014. *The SAGE Encyclopedia of Action Research Chapter Title: "Data Analysis".* London: SAGE Publications Ltd.

JIANG, R., WU, X. and BHARGAVA, B., 2016. SDSS-MAC: Secure data sharing scheme in multi-authority cloud storage systems. *Computers & Security,* **62**, pp. 193-212.

JOHANNESSON, P. and PERJONS, E., 2014. *An introduction to design science.* Springer.

K. HAUFE, S. DZOMBETA, K. BRANDIS, V. STANTCHEV and R. COLOMO-PALACIOS, 2018. Improving Transparency and Efficiency in IT Security Management Resourcing. *IT Professional,* **20**(1), pp. 53-62.

K. M. KHAN and YUN BAI, 2013. Automatic verification of health regulatory compliance in cloud computing, *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)* 2013, pp. 719-721.

K. SONI and S. KUMAR, 2019. *Comparison of RBAC and ABAC Security Models for Private Cloud.*

KAMOCKI, P. and WITT, A., 2020. Privacy by Design and Language Resources, *Proceedings of The 12th Language Resources and Evaluation Conference* 2020, pp. 3423-3427.

KAZI, A.M. and KHALID, W., 2012. Questionnaire designing and validation. *Journal of the Pakistan Medical Association,* **62**(5), pp. 514.

KOGAN, A., MAYHEW, B.W. and VASARHELYI, M.A., 2019. Audit data analytics research—An application of design science methodology. *Accounting Horizons,* **33**(3), pp. 69-73.

KOMU, M., SETHI, M., MALLAVARAPU, R., OIROLA, H., KHAN, R. and TARKOMA, S., 2012. Secure Networking for Virtual Machines in the Cloud, *2012 IEEE International Conference on Cluster Computing Workshops*, Sept 2012, pp. 88-96.

KULKARNI, G., KHATAWKAR, P., SHELKE, R., SOLANKE, V. and WAGHMARE, R., 2013. “Multi-tenant SaaS cloud”, *2013 Africon*, Sept 2013, pp. 1-4.

KUMAR, R., 2018. *Research methodology: A step-by-step guide for beginners.* Sage.

KUMARAGURU, P., CRANOR, L., LOBO, J. and CALO, S., 2007. A survey of privacy policy languages, *Workshop on Usable IT Security Management (USM 07): Proceedings of the 3rd Symposium on Usable Privacy and Security, ACM* 2007.

KUNG, A., KARGL, F., SUPPAN, S., CUELLAR, J., PÖHLS, H.C., KAPOVITS, A., MCDONNELL, N.N. and MARTIN, Y.S., 2017. A privacy engineering framework for the internet of things. *Data Protection and Privacy:(In) visibilities and Infrastructures.* Springer, pp. 163-202.

L. C. OCHEI, J. M. BASS and A. PETROVSKI, 2015. *Evaluating Degrees of Multitenancy Isolation: A Case Study of Cloud-Hosted GSD Tools.*

L. ELLURI, A. NAGAR and K. P. JOSHI, 2018a. An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance, *2018 IEEE International Conference on Big Data (Big Data)* 2018a, pp. 1266-1271.

L. ELLURI, A. NAGAR and K. P. JOSHI, 2018b. An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance, *2018 IEEE International Conference on Big Data (Big Data)* 2018b, pp. 1266-1271.

L. LI, Y. WANG, Y. DING and Y. ZHANG, 2015. Multi-tenants Data Duplication Secure Storage in SaaS, *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* 2015, pp. 233-238.

LARSEN, P.G., LAUSDAHL, K., BATTLE, N., FITZGERALD, J., WOLFF, S., SAHARA, S., VERHOEF, M., TRAN-JØRGENSEN, P.W., ODA, T. and CHISHOLM, P., 2010. VDM-10 language manual. *The Overture Open Source Initiative, Tech.Rep.TR-2010-06,* .

LAUER, D.A. and PENTAK, S., 2011. *Design basics.* Cengage Learning.

LI, Z.S., WERNER, C. and ERNST, N., 2019. Continuous Requirements: An Example Using GDPR, *2019 IEEE 27th International Requirements Engineering Conference Workshops (REW)* 2019, IEEE, pp. 144-149.

LI, Z.S., WERNER, C., ERNST, N. and DAMIAN, D., 2020. GDPR Compliance in the Context of Continuous Integration. *arXiv preprint arXiv:2002.06830,* .

LÓPEZ-VIANA, R., DÍAZ, J., DÍAZ, V.H. and MARTÍNEZ, J., 2020. Continuous delivery of customized SaaS edge applications in highly distributed IoT systems. *IEEE Internet of Things Journal,* **7**(10), pp. 10189-10199.

LOUKIS, E., JANSSEN, M. and MINTCHEV, I., 2019. Determinants of software-as-a-service benefits and impact on firm performance. *Decision Support Systems,* **117**, pp. 38-47.

LUKYANENKO, R. and PARSONS, J., 2013. Reconciling theories with design choices in design science research, *International Conference on Design Science Research in Information Systems* 2013, Springer, pp. 165-180.

M. ED-DAIBOUNI, A. LEBBAT, S. TALLAL and H. MEDROMI, 2016. A formal specification approach of Privacy-aware Attribute Based Access Control (Pa-ABAC) model for cloud computing, *2016 Third International Conference on Systems of Collaboration (SysCo)* 2016, pp. 1-5.

M. G. JAATUN, I. A. TØNDEL, N. B. MOE, D. S. CRUZES, K. BERNSMED and B. HAUGSET, 2017. Accountability Requirements for the Cloud, *2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)* 2017, pp. 375-382.

M. HASHEM EIZA and Q. NI, 2017. *Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity.*

M. M. KRUPP, M. RUEBEN, C. M. GRIMM and W. D. SMART, 2017. A focus group study of privacy concerns about telepresence robots, *2017 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)* 2017, pp. 1451-1458.

M. OLURIN, C. ADAMS and L. LOGRIPPO, 2012. Platform for privacy preferences (P3P): Current status and future directions, *2012 Tenth Annual International Conference on Privacy, Security and Trust* 2012, pp. 217-220.

M. REZAEI-MALEK, N. REZAEI-MALEK and R. TAVAKKOLI-MOGHADDAM, 2013. *Improving performance of customer relationship management by knowledge management — A case study.*

M. S. FERDOUS and R. POET, 2014. CAFS: A Framework for Context-Aware Federated Services, *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* 2014, pp. 130-139.

M. UDDIN, S. ISLAM and A. AL-NEMRAT, 2019. *A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control.*

MAGUIRE, M. and DELAHUNT, B., 2017. Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education,* **9**(3),.

MAJDA, E. and AHMED, E., 2015. Using cloud SaaS to ensure interoperability and standardization in heterogeneous Cloud based environment, *2015 5th World Congress on Information and Communication Technologies (WICT)*, Dec 2015, pp. 29-34.

MANOVICH, L., 2011. Trending: The promises and the challenges of big social data. *Debates in the digital humanities,* **2**(1), pp. 460-475.

MARGULIS, S.T., 2003. Privacy as a social issue and behavioral concept. *Journal of Social Issues,* **59**(2), pp. 243-261.

MARIA, K., 2020-last update, California Consumer Privacy Act (CCPA): What you need to know to be compliant. Available: https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html.

MARKOPOULOU, D., PAPAKONSTANTINOU, V. and DE HERT, P., 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review,* **35**(6), pp. 105336.

MARTÍN, Y., DEL ALAMO, J.M. and YELMO, J.C., 2014. Engineering privacy requirements valuable lessons from another realm, *2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)* 2014, IEEE, pp. 19-24.

MCCARTHY, J., 2007. What is artificial intelligence? .

MONDAY.COM, 2020-last update, About Us. Available: https://monday.com/about.

MORABITO, R., COZZOLINO, V., DING, A.Y., BEIJAR, N. and OTT, J., 2018. Consolidate IoT edge computing with lightweight virtualization. *Ieee network,* **32**(1), pp. 102-111.

MORENO-VOZMEDIANO, R., MONTERO, R.S. and LLORENTE, I.M., 2013. Key Challenges in Cloud Computing: Enabling the Future Internet of Services. *IEEE Internet Computing,* **17**(4), pp. 18-25.

MOUDRA, K., SVOBODOVA, L., FOLTÝNOVÁ, H.B. and PŘIBYL, O., 2020. Effects of Focus Groups' results on a Travel Behavior Survey design, *2020 Smart City Symposium Prague (SCSP)* 2020, IEEE, pp. 1-6.

MULLARKEY, M.T. and HEVNER, A.R., 2019. An elaborated action design research process model. *European Journal of Information Systems,* **28**(1), pp. 6-20.

N. KSHETRI and S. MURUGESAN, 2013. Cloud Computing and EU Data Privacy Regulations. *Computer,* **46**(3), pp. 86-89.

NAGANO, M., ARAI, Y., FUJIHASHI, T., WATANABE, T. and SARUWATARI, S., 2021. Design and Implementation of Device Monitoring SaaS for DIY-IoT Systems, *2021 IEEE International Conference on Consumer Electronics (ICCE)* 2021, IEEE, pp. 1-4.

NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY -USA, 2011. *The NIST Definition of Cloud Computing.* US: US Department of Commerce.

NAVIMIPOUR, N.J., 2015. A formal approach for the specification and verification of a trustworthy human resource discovery mechanism in the expert cloud. *Expert Systems with Applications,* **42**(15-16), pp. 6112-6131.

NI LOIDEAIN, N., 2016. The end of safe harbor: Implications for EU digital privacy and data protection law. *Journal of Internet Law,* **19**(8),.

NIGERIAN INFORMATION TECHNOLOGY DEVELOPMENT AGENCY, April, 25 2019, 2019-last update, The Nigerian Data Protection Regulation, 2019. Available: https://nitda.gov.ng/wp-content/.../Nigeria%20Data%20Protection%20Regulation.pdf.

NIST GUIDE, December 2011, , NIST Security and Privacy Guide in Cloud Computing.

NITDA, N., 2019-last update, List of Licensed Data Protection Compliance organisations (DPCO). Available: https://nitda.gov.ng/nit/list-of-licensed-data-protection-compliance-organisations-dpco/.

NOTARIO, N., CRESPO, A., MARTÍN, Y., DEL ALAMO, J.M., LE MÉTAYER, D., ANTIGNAC, T., KUNG, A., KROENER, I. and WRIGHT, D., 2015. PRIPARE: integrating privacy best practices into a privacy engineering methodology, *2015 IEEE Security and Privacy Workshops* 2015, IEEE, pp. 151-158.

O. ETHELBERT, F. F. MOGHADDAM, P. WIEDER and R. YAHYAPOUR, 2017. *A JSON Token-Based Authentication and Access Management Schema for Cloud SaaS Applications.*

O'REGAN, G., 2017. Z formal specification language. *Concise Guide to Formal Methods.* Springer, pp. 155-171.

OASIS, 2017, 2017-last update, eXtensible Access Control Markup Language (XACML) Version 3.0 2017. Available: http://docs.oasis-open.org/xacml/3.0/errata01/os/xacml-3.0-core-spec-errata01-os.html.

O'BRIEN, D. and TORRES, A.M., 2012. Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management,* .

OFFSHORE ENGINEER, 2020-last update, Shell Taps Kongsberg for Cloud-Based Digital Twin Services. Available: https://www.oedigital.com/news/481298-shell-taps-kongsberg-for-cloud-based-digital-twin-services.

P. BALLARINI, M. BATTEUX, L. CHARTIER and A. RAUZY, 2018. Analysis of business process specifications with OpenAltarica, *2018 IEEE International Systems Engineering Symposium (ISSE)* 2018, pp. 1-8.

P. HARIKRISHNA and A. AMUTHAN, 2016. A survey of testing as a service in cloud computing, *2016 International Conference on Computer Communication and Informatics (ICCCI)* 2016, pp. 1-5.

P. XU, T. JIAO, Q. WU, W. WANG and H. JIN, 2016. *Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email.*

PANDIT, H.J., O'SULLIVAN, D. and LEWIS, D., 2018. Queryable provenance metadata For GDPR compliance. *Procedia Computer Science,* **137**, pp. 262-268.

PAPADIMITRIOU, S., MOUGIAKOU, E. and VIRVOU, M., 2019. Smart educational games and Consent under the scope of General Data Protection Regulation, *2019 10th International Conference on Information, Intelligence, Systems and Applications (IISA)*, July 2019, pp. 1-8.

PARK, S., HWANG, M., LEE, S. and PARK, Y.B., 2015. A Generic Software Development Process Refined from Best Practices for Cloud Computing. *Sustainability,* **7**(5), pp. 5321-5344.

PARNAS, D.L., 2010. Really rethinking'formal methods'. *Computer,* **43**(1), pp. 28-34.

PAT BAZELEY AND KRISTI JACKSON, 2013. *Qualitative Data Analysis with Nvivo.* 2nd edn. London: Sage.

PERRONS, R.K. and HEMS, A., 2013. *Cloud computing in the upstream oil & gas industry: A proposed way forward.*

PHELPS, J., NOWAK, G. and FERRELL, E., 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing,* **19**(1), pp. 27-41.

POROOR, J. and JAYARAMAN, B., 2012. *C2L:A Formal Policy Language for Secure Cloud Configurations.*

Q. DONG, D. HUANG, J. LUO and M. KANG, 2018. *Achieving Fine-Grained Access Control with Discretionary User Revocation over Cloud Data.*

Q. ZHANG, S. WANG, D. ZHANG, J. WANG and Y. ZHANG, 2019. *Time and Attribute Based Dual Access Control and Data Integrity Verifiable Scheme in Cloud Computing Applications.*

QUALTRICS, 2017. *2017 SaaS Security Study.*

R. MAHESHWARI, A. TOSHNIWAL and A. DUBEY, 2020. Software As A Service Architecture and its Security Issues: A Review, *2020 Fourth International Conference on Inventive Systems and Control (ICISC)* 2020, pp. 766-770.

RADICATI, S. and LEVENSTEIN, J., 2013. Email statistics report, 2013-2017. *The Radicati Group, Inc., Tech.Rep,* .

RAJESWARI, S. and KALAISELVI, R., 2017. Survey of data and storage security in cloud computing, *2017 IEEE International Conference on Circuits and Systems (ICCS)*, Dec 2017, pp. 76-81.

RANDOLPH, J., 2009. A guide to writing the dissertation literature review. *Practical Assessment, Research, and Evaluation,* **14**(1), pp. 13.

RANTANEN, M.M., NASKALI, J., KIMPPA, K.K. and KOSKINEN, J., 2020. Ethical Justification of the Value Basis of the European Data Economy Ecosystems. *Tethics* 2020, pp. 70-85.

RASHMI, DR SAHOO, G, DR MEHFUZ, S, 2013. Securing Software as a Service Model of CloudComputing:Issues and Solutions. **Vol.3,**(No.4), pp. 1-11.

RIEMER, K. and JOHNSTON, R.B., 2014. Rethinking the place of the artefact in IS using Heidegger's analysis of equipment. *European Journal of Information Systems,* **23**(3), pp. 273-288.

ROOPA, S. and RANI, M., 2012. Questionnaire designing for a survey. *Journal of Indian Orthodontic Society,* **46**(4_suppl1), pp. 273-277.

ROSENBLUM, D., 2007. What anyone can know: The privacy risks of social networking sites. *IEEE Security & Privacy,* **5**(3), pp. 40-49.

RUSSELL, K.D., O'RAGHALLAIGH, P., O'REILLY, P. and HAYES, J., 2018. Digital privacy GDPR: a proposed digital transformation framework, *AMCIS 2018-24th Americas Conference on Information Systems* 2018, Association for Information Systems, pp. 1-10.

S. ALEEM, F. AHMED, R. BATOOL and A. KHATTAK, 2019. *Empirical Investigation of Key Factors for SaaS Architecture Dimension.*

S. KURJAKOVIC and K. HINKELMANN, 2018. Enterprise Architecture Driven and User-Friendly SaaS Service Selection, *2018 Sixth International Conference on Enterprise Systems (ES)* 2018, pp. 196-203.

S. LIEBESMAN, 2002. ISO 9000:2000-the challenges and opportunities for internal auditors, *Annual Reliability and Maintainability Symposium. 2002 Proceedings (Cat. No.02CH37318)* 2002, pp. 480-483.

S. LINS, S. SCHNEIDER and A. SUNYAEV, 2018. Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing. *IEEE Transactions on Cloud Computing,* **6**(3), pp. 890-903.

S. M. N. ISLAM and M. M. RAHMAN, 2017. Securing virtual machine images of cloud by encryption through Kerberos, *2017 2nd International Conference for Convergence in Technology (I2CT)* 2017, pp. 1074-1079.

S. S. GHUGE, N. KUMAR, S. SAVITHA and V. SURAJ, 2020. Multilayer Technique to Secure Data Transfer in Private Cloud for SaaS Applications, *2020 2nd International*

Conference on Innovative Mechanisms for Industry Applications (ICIMIA) 2020, pp. 646-651.

S. TRABELSI, J. SENDOR and S. REINICKE, 2011. PPL: PrimeLife Privacy Policy Engine, *2011 IEEE International Symposium on Policies for Distributed Systems and Networks* 2011, pp. 184-185.

S. WANG, J. ZHOU, J. K. LIU, J. YU, J. CHEN and W. XIE, 2016. *An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing.*

S. XIONG, Q. NI, L. WANG and Q. WANG, 2020. *SEM-ACSIT: Secure and Efficient Multiauthority Access Control for IoT Cloud Storage.*

S. YULIANTO, C. LIM and B. SOEWITO, 2016. Information security maturity model: A best practice driven approach to PCI DSS compliance, *2016 IEEE Region 10 Symposium (TENSYMP)* 2016, pp. 65-70.

SALAMI, E., 2020. Fingerprint Generated Data: An Evaluation of the Efficacy of the Nigerian Data Protection Regulation. *Computer and telecommunications law review,* **26**(7), pp. 184-191.

SARATHA, P., UMA, G. and SANTHOSH, B., 2017. Formal specification for online food ordering system using z language, *2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)* 2017, IEEE, pp. 343-348.

SARKAR, S., BANATRE, J., RILLING, L. and MORIN, C., 2018. Towards Enforcement of the EU GDPR: Enabling Data Erasure, *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, July 2018, pp. 222-229.

SATRJEENPONG, P.S., TAPURIA, A., CURCIN, V. and KALRA, D., 2018. Identifying audit trail viewer requirements for user-focused design: a qualitative focus group study, *2018 IEEE International Conference on Healthcare Informatics (ICHI)* 2018, IEEE, pp. 405-406.

SCHAAR, P., 2010. Privacy by design. *Identity in the Information Society,* **3**(2), pp. 267-274.

SCHOBBENS, P., HEYMANS, P. and TRIGAUX, J., 2006. Feature diagrams: A survey and a formal semantics, *14th IEEE International Requirements Engineering Conference (RE'06)* 2006, IEEE, pp. 139-148.

SERNA, E. and SERNA, A., 2017. Power and limitations of formal methods for software fabrication: Thirty years later. *Informatica,* **41**(3),.

SERRADO, J., PEREIRA, R.F., DA SILVA, M.M. and BIANCHI, I.S., 2020. Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy, Regulation and Governance,* .

SHAOYING LIU and R. ADAMS, 1995. Limitations of formal methods and an approach to improvement, - *Proceedings 1995 Asia Pacific Software Engineering Conference* 1995, pp. 498-507.

SINGH, A. and CHATTERJEE, K., 2017. *Cloud security issues and challenges: A survey.*

SINGH, S., JEONG, Y. and PARK, J.H., 2016. *A survey on cloud computing security: Issues, threats, and solutions.*

SION, L., DEWITTE, P., LANDUYT, D.V., WUYTS, K., EMANUILOV, I., VALCKE, P. and JOOSEN, W., 2019. An Architectural View for Data Protection by Design, *2019 IEEE International Conference on Software Architecture (ICSA)*, March 2019, pp. 11-20.

SKENDŽIĆ, A., KOVAČIĆ, B. and TIJAN, E., 2018. General data protection regulation — Protection of personal data in an organisation, *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2018, pp. 1370-1375.

SLIM TRABELSI , AKRAM NJEH , LAURENT BUSSARD , GREGORY NEVEN, 2010. *PPL Engine: A Symmetric Architecture for Privacy Policy Handling* .

SMITH, H.J., DINEV, T. and XU, H., 2011. Information privacy research: an interdisciplinary review. *MIS quarterly,* , pp. 989-1015.

SOLOVE, D.J., 2005. A taxonomy of privacy. *U.Pa.L.Rev.,* **154**, pp. 477.

SONI, D. and KUMAR, M., 2017. Secure data communication in client-cloud environment: A survey, *2017 7th International Conference on Communication Systems and Network Technologies (CSNT)*, Nov 2017, pp. 246-252.

SONI, R., AMBALKAR, S. and BANSAL, P., 2016. Security and privacy in cloud computing, *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, March 2016, pp. 1-6.

SOUAF, S., BERTHOMÉ, P. and LOULERGUE, F., 2018. A cloud brokerage solution: formal methods meet security in cloud federations, *2018 International Conference on High Performance Computing & Simulation (HPCS)* 2018, IEEE, pp. 691-699.

SOURI, A., NAVIMIPOUR, N.J. and RAHMANI, A.M., 2018. Formal verification approaches and standards in the cloud computing: a comprehensive and systematic review. *Computer Standards & Interfaces,* **58**, pp. 1-22.

SPIEKERMANN, S., 2012. The challenges of privacy by design. *Communications of the ACM,* **55**(7), pp. 38-40.

SPIEKERMANN, S., KORUNOVSKA, J. and LANGHEINRICH, M., 2018. Inside the organization: Why privacy and security engineering is a challenge for engineers. *Proceedings of the IEEE,* **107**(3), pp. 600-615.

STAVRINIDES, G.L. and KARATZA, H.D., 2017. The impact of data locality on the performance of a SaaS cloud with real-time data-intensive applications, *2017 IEEE/ACM 21st International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, Oct 2017, pp. 1-8.

SUBASHINI, S. and KAVITHA, V., 2011. *A survey on security issues in service delivery models of cloud computing.*

SUEN, C.H., KO, R.K., TAN, Y.S., JAGADPRAMANA, P. and LEE, B.S., 2013. S2logger: End-to-end data tracking mechanism for cloud data provenance, *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* 2013, IEEE, pp. 594-602.

SULTAN A, W.A., 2016. Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solution. **Vol. 7**(No. 4, 2016), pp. 485-498.

SURYA, K., NIVEDITHAA, M., UMA, S. and VALLIYAMMAI, C., 2013. Security issues and challenges in cloud, *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, Dec 2013, pp. 889-893.

T. INDHUMATHIL, N. AARTHY, V. D. DEVI and V. N. SAMYUKTHA, 2017. Third-party auditing for cloud service providers in multicloud environment, *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)* 2017, pp. 347-352.

T. KITTMANN, J. LAMBRECHT and C. HORN, 2018. A privacy-aware distributed software architecture for automation services in compliance with GDPR, *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)* 2018, pp. 1067-1070.

TAKABI, H., JOSHI, J.B.D. and AHN, G.J., 2010. Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security Privacy,* **8**(6), pp. 24-31.

TAMBURRI, D.A., 2019. *Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation.*

TAN, X. and AI, B., 2011. The issues of cloud computing security in high-speed railway, *Proceedings of 2011 International Conference on Electronic Mechanical Engineering and Information Technology*, Aug 2011, pp. 4358-4363.

TERZO, O., RUIU, P., BUCCI, E. and XHAFA, F., 2013. Data as a service (DaaS) for sharing and processing of large data collections in the cloud, *2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems* 2013, IEEE, pp. 475-480.

THE UK CARDS ASSOCIATION, 2018-last update, **What is PCI DSS?**. Available: http://www.theukcardsassociation.org.uk/security/What_is_PCI%20DSS.asp.

TIWARI, P.K. and JOSHI, S., 2014a. A review of data security and privacy issues over SaaS, *2014 IEEE International Conference on Computational Intelligence and Computing Research*, Dec 2014a, pp. 1-6.

TIWARI, P.K. and JOSHI, S., 2014b. A review of data security and privacy issues over SaaS, *2014 IEEE International Conference on Computational Intelligence and Computing Research*, Dec 2014b, pp. 1-6.

TRAPERO, R., MODIC, J., STOPAR, M., TAHA, A. and SURI, N., 2017. *A novel approach to manage cloud security SLA incidents.*

TRUECALLER, 29/01/2020, 2020-last update, About Trucaller: Making communication safe and efficient. Available: https://www.truecaller.com/about.

UK DATA ARCHIVE, 2007-last update. Available: https://data-archive.ac.uk/media/285633/ukda-example-transcription-instructions.pdf.

VAN DER SLOOT, B., 2017. Decisional privacy 2.0: the procedural requirements implicit in Article 8 ECHR and its potential impact on profiling. *International Data Privacy Law,* **7**(3), pp. 190-201.

VARADHARAJAN, V. and TUPAKULA, U., 2016. Securing Services in Networked Cloud Infrastructures. *IEEE Transactions on Cloud Computing,* , pp. 1-1.

VERDOUW, C.N., WOLFERT, J., BEULENS, A. and RIALLAND, A., 2016. Virtualization of food supply chains with the internet of things. *Journal of Food Engineering,* **176**, pp. 128-136.

VIDHYALAKSHMI, R. and KUMAR, V., 2014. Design comparison of traditional application and SaaS, *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, March 2014, pp. 541-544.

VINCENT, O., 2020. Data Privacy and Protection: The Role of Regulation and Implications for Data Controllers in Developing Countries, *Information and Communication Technologies for Development: 16th IFIP WG 9.4 International Conference on Social Implications of Computers in Developing Countries, ICT4D 2020, Manchester, UK, June 10–11, 2020, Proceedings* 2020, Springer Nature, pp. 205.

VINH THONG TA, May 15, 2018. Privacy by Design: On the Formal Design and Conformance
Check of Personal Data Protection Policies and Architectures.

VOLLMER, N., 2018. *Recital 71 EU general data protection regulation (EU-GDPR),* .

W. STALLINGS, 2020a. *Handling of Personal Information and Deidentified, Aggregated, and Pseudonymized Information Under the California Consumer Privacy Act.*

W. STALLINGS, 2020b. *Handling of Personal Information and Deidentified, Aggregated, and Pseudonymized Information Under the California Consumer Privacy Act.*

WANG, Y.H., 2011a. The role of SaaS privacy and security compliance for continued SaaS use, *The 7th International Conference on Networked Computing and Advanced Information Management*, June 2011a, pp. 303-306.

WANG, Y.H., 2011b. The role of SaaS privacy and security compliance for continued SaaS use, *The 7th International Conference on Networked Computing and Advanced Information Management*, June 2011b, pp. 303-306.

WARREN, S.D. and BRANDEIS, L.D., 1890. The right to privacy. *Harvard law review,* , pp. 193-220.

WARREN, S. and BRANDEIS, L., 2019. *The right to privacy.* Litres.

WEBER, R., 2011. The information systems discipline: the need for and nature of a foundational core. *Information Systems,* .

WESTIN, A.F., 1968. Privacy and freedom. *Washington and Lee Law Review,* **25**(1), pp. 166.

WIERINGA, R.J., 2014. *Design science methodology for information systems and software engineering.* Springer.

WRAY, N., MARKOVIC, M. and MANDERSON, L., 2007. “Researcher saturation”: the impact of data triangulation and intensive-research practices on the researcher and qualitative research process. *Qualitative health research,* **17**(10), pp. 1392-1402.

X. ZHENG, J. JIANG, Y. ZHANG, Y. DENG, M. FU, T. ZHENG and X. LIU, 2017. SmartVM: A Multi-Layer Microservice-Based Platform for Deploying SaaS, *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)* 2017, pp. 470-474.

XU, H., DINEV, T., SMITH, J. and HART, P., 2011. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems,* **12**(12), pp. 1.

Y. LIU, K. XU and J. SONG, 2013. *A Task-Attribute-Based Workflow Access Control Model.*

Y. WANG, Y. MA, K. XIANG, Z. LIU and M. LI, 2018. A Role-Based Access Control System Using Attribute-Based Encryption, *2018 International Conference on Big Data and Artificial Intelligence (BDAI)* 2018, pp. 128-133.

YANG, K. and JIA, X., 2013. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. *IEEE Transactions on Parallel and Distributed Systems,* **24**(9), pp. 1717-1726.

YIMAM, D. and FERNANDEZ, E.B., 2016. A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications,* **7**(1), pp. 5.

YU, S., WANG, G., LIU, X. and NIU, J., 2018. Security and privacy in the age of the smart internet of things: An overview from a networking perspective. *IEEE Communications Magazine,* **56**(9), pp. 14-18.

YU, T. and WINSLETT, M., 2003. Policy migration for sensitive credentials in trust negotiation, *Proceedings of the 2003 ACM workshop on Privacy in the electronic society* 2003, pp. 9-20.

Z. ISMAIL, C. KIENNERT, J. LENEUTRE and L. CHEN, 2016a. Auditing a Cloud Provider's Compliance With Data Backup Requirements: A Game Theoretical Analysis. *IEEE Transactions on Information Forensics and Security,* **11**(8), pp. 1685-1699.

Z. ISMAIL, C. KIENNERT, J. LENEUTRE and L. CHEN, 2016b. Auditing a Cloud Provider's Compliance With Data Backup Requirements: A Game Theoretical Analysis. *IEEE Transactions on Information Forensics and Security,* **11**(8), pp. 1685-1699.

ZHOU, M., ZHANG, R., XIE, W., QIAN, W. and ZHOU, A., 2010. Security and Privacy in Cloud Computing: A Survey, *2010 Sixth International Conference on Semantics, Knowledge and Grids*, Nov 2010, pp. 105-112.

ZHU, Y., HUANG, D., HU, C. and WANG, X., 2014. From RBAC to ABAC: constructing flexible data access control for cloud storage services. *IEEE Transactions on Services Computing,* **8**(4), pp. 601-616.

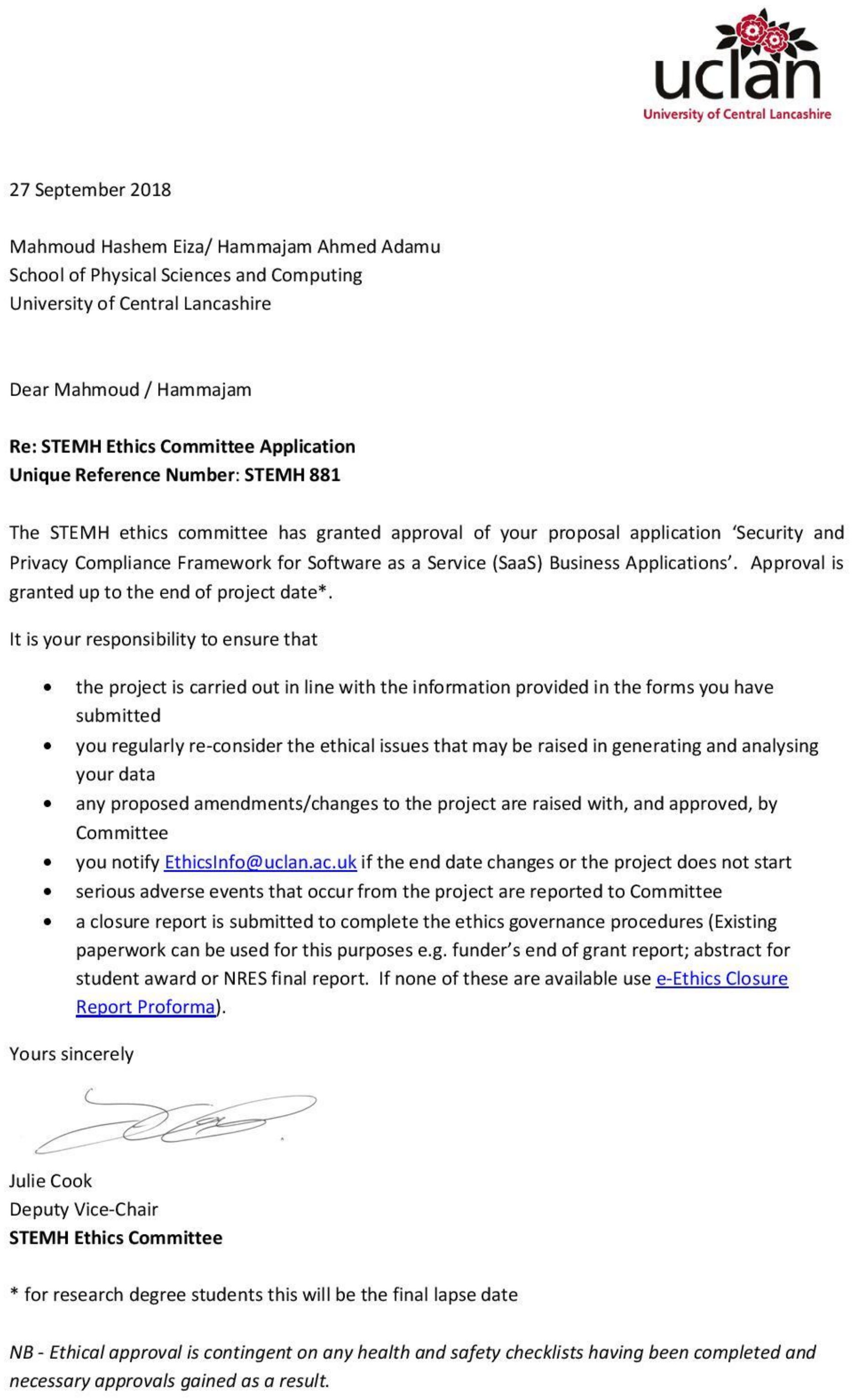
ZISSIS, D. and LEKKAS, D., 2012. *Addressing cloud computing security issues.*

Appendix 1: SaaS-PPL extended Triggers, Actions, Conditions and Obligations

Case	Trigger	Action	Obligation
Case 1.0 Personal Data Collection-Consent Collection	$TriggerCollectPersonalData(typeset, time)$	$ActionCollectConsent(typeset, time - value)$	Do $ActionCollectConsent(typeset, time - tvalue)$ when $TriggerCollectPersonalData(typeset, time)$
Case 1.1 Personal Data: Purpose of Data Collection	$TriggerCollectPurposes(typeset, purposes)$	**Condition** for Purpose: $SubsetOf\ (purposes, cpurp)$	$When\ TriggerCollectPersonalData(typeset, purposes)$, then $SubsetOf\ (purposes, cpurp)$
Case 2.0 Personal Data Processing Consent Collection	$TriggerProcessPersonalData\ (typeset,\ time)$	$ActionProcessConsent\ (typeset,\ time\ tvalue)$	Do $ActionProcessConsent\ (typeset,\ time\ tvalue)$ when $TriggerProcessData\ (typeset,\ time\ tvalue)$
Case 2.1 Personal Data Processing Purpose	$TriggerProcessPersonalData\ (typeset\ , purposes)$	**Condition** for Purpose: $SubsetOf\ (purposes, procpurp)$	$When\ TriggerProcessPersonalData\ (typeset\ , purposes)$, then $SubsetOf\ (purposes, procpurp)$
Case 2.2 Personal Data Processing whocanproc	$TriggerProcessPersonalData\ (typeset, processby)$	**Condition** for $whocanproc$: $SubsetOf\ (processby, whocanproc)$	$When\ TriggerProcessPersonalData\ (typeset, processby)$, then $SubsetOf\ (processby, whocanproc)$
Case 2.3 Personal Data Processing – Notification	$TriggerProcessPersonalData\ (typeset, time)$	$ActionProcessNotification\ (typeset, time - tvalue\ )$	Do $ActionProcessNotification\ (typeset, time - tvalue\ )$ when $TriggerProcessPersonalData\ (typeset, time - tvalue\ )$
Case 3.0 Personal Data Storage Obligation Encrypted	$TriggerStoreData\ (typeset, time)$	$ActionSaveEncryptedData\ (typeset, spkey, SpOwnServer, time)$	Do $ActionSaveEncryptedData\ (typeset, spkey, SpOwnServer, time)$ when $TriggerStoreData\ (typeset, time)$
Case 3.1 Personal Data Storage Obligation – Saved in Plain Text	$TriggerStoreData\ (typeset, time)$	$ActionSavePlainData\ (\ typeset, SpOwnServer, time\ )$	Do $ActionSavePlainData\ (\ typeset, SpOwnServer, time\ )$ when $TriggerStoreData\ (typeset, time)$
Case 3.2 Personal Data Storage Obligation – *howstore* Hidden	$TriggerStoreData\ (typeset, time)$	$ActionSaveEncryptedData\ (typeset, notspkey, SpOwnServer$	Do $ActionSaveEncryptedData\ (typeset, notspkey, SpOwnServer, ti$, when $TriggerStoreData\ (typeset, time)$

Case 3.3 Personal Data Storage Obligation – *howstore* Available	$TriggerStoreData\ (typeset, time)$	*ActionSaveEncryptedData (typeset, spkey, 3rdPartyServers, time)*	$Do\ ActionSaveEncryptedData\ (typeset, spkey, 3rdPartyServers, ti$ $when\ TriggerStoreData\ (typeset, time)$
Case 3.4 Personal Data Storage Obligation – ***howstore* Clientpla**	$TriggerStoreData\ (typeset, time)$	*ActionSaveEncryptedData (typeset, notspkey,* $clientplace,$ *time)*	$Do\ ActionSaveEncryptedData\ (typeset, notspkey, clientplace, time$ $TriggerStoreData(typeset, time)$
Case 4.1 Personal Data Retention – Notification	$TriggerRetentionPersonalData\ (typeset, time)$	$ActionRetentiontionNotification(typeset, time - tvalue\ )$	*Do* $ActionRetentionNotification(typeset, time - tvalue) when\ TriggerRetentionPersonalData\ (typeset, time)$
Case 4.2 Personal Data Retention Obligation – Trigger Data Retention	$TriggerInitiateRetentionData\ (typeset, time1)$	$ActionDataRetention(typeset, fromwhere, time2, [time1, tim$ $+ dd])$	*Do* $ActionDataRetention(typeset, fromwhere, time2, [time1, time1 + dd])\ \ When\ TriggerInitiateRetentionData(typeset, time1)$
Case 4.3 Personal Data Retention Obligation – Trigger Data Retention - Global delay	$TriggerUnregister\ (typeset, time1)$	$ActionDataRetention\ (typeset, fromwhere, time2, [time1, tin$ $+ gd])$	*Do* $ActionDataRetention(typeset, fromwhere, time2, [time1, time1 + gd])\ When\ TriggerUnregister\ (typeset, time1)$
Case 5.0 Personal Data Forwarding Obligation – Consent	$TriggerForwardPersonalData(typeset, time)$	$ActionCollectConsent(typeset, time - value)$	*Do* $ActionCollectConsent(typeset, time - value) when\ TriggerForwardPersonalData(typeset, time)$
Case 5.1 Personal Data Forwarding Obligation – Purpose	$TriggerForwardingPurposes(typeset, purpose$	*Collection **Condition** for Purpose:* $SubsetOf\ \ (purposes, fwpurp)$	$When\ TriggerForwardPersonalData(typeset, purposes)\ then$ $SubsetOf\ \ (purposes, fwpurp)$
Case 5.2 Personal Data Forwarding Obligation – Third-party List	$TriggerForward3rdPartyRecipient\ (typeset, 3$	***Condition** for 3rdpartyForwarding:* $SubsetOf\ \ (purposes, fwpurp, fw3rdParty)$	$When\ TriggerForwardPersonalData(typeset,),$*then* $SubsetOf\ \ (purposes, fwpurp, 3rdParty)$
Case 5.3 Personal Data Forwarding Obligation – Notification	$TriggerForwardPersonalData\ (typeset, time)$	$ActionDeletionNotification\ (typeset, time - tvalue\ )$	*Do* $ActionForwardingNotification\ (typeset, time - tvalue)\ when\ TriggerForwardingPersonalData(typeset, time$

Appendix 2: Ethical Approval



uclan
University of Central Lancashire

27 September 2018

Mahmoud Hashem Eiza/ Hammajam Ahmed Adamu
School of Physical Sciences and Computing
University of Central Lancashire

Dear Mahmoud / Hammajam

Re: STEMH Ethics Committee Application
Unique Reference Number: **STEMH 881**

The STEMH ethics committee has granted approval of your proposal application 'Security and Privacy Compliance Framework for Software as a Service (SaaS) Business Applications'. Approval is granted up to the end of project date*.

It is your responsibility to ensure that

- the project is carried out in line with the information provided in the forms you have submitted
- you regularly re-consider the ethical issues that may be raised in generating and analysing your data
- any proposed amendments/changes to the project are raised with, and approved, by Committee
- you notify EthicsInfo@uclan.ac.uk if the end date changes or the project does not start
- serious adverse events that occur from the project are reported to Committee
- a closure report is submitted to complete the ethics governance procedures (Existing paperwork can be used for this purposes e.g. funder's end of grant report; abstract for student award or NRES final report. If none of these are available use e-Ethics Closure Report Proforma).

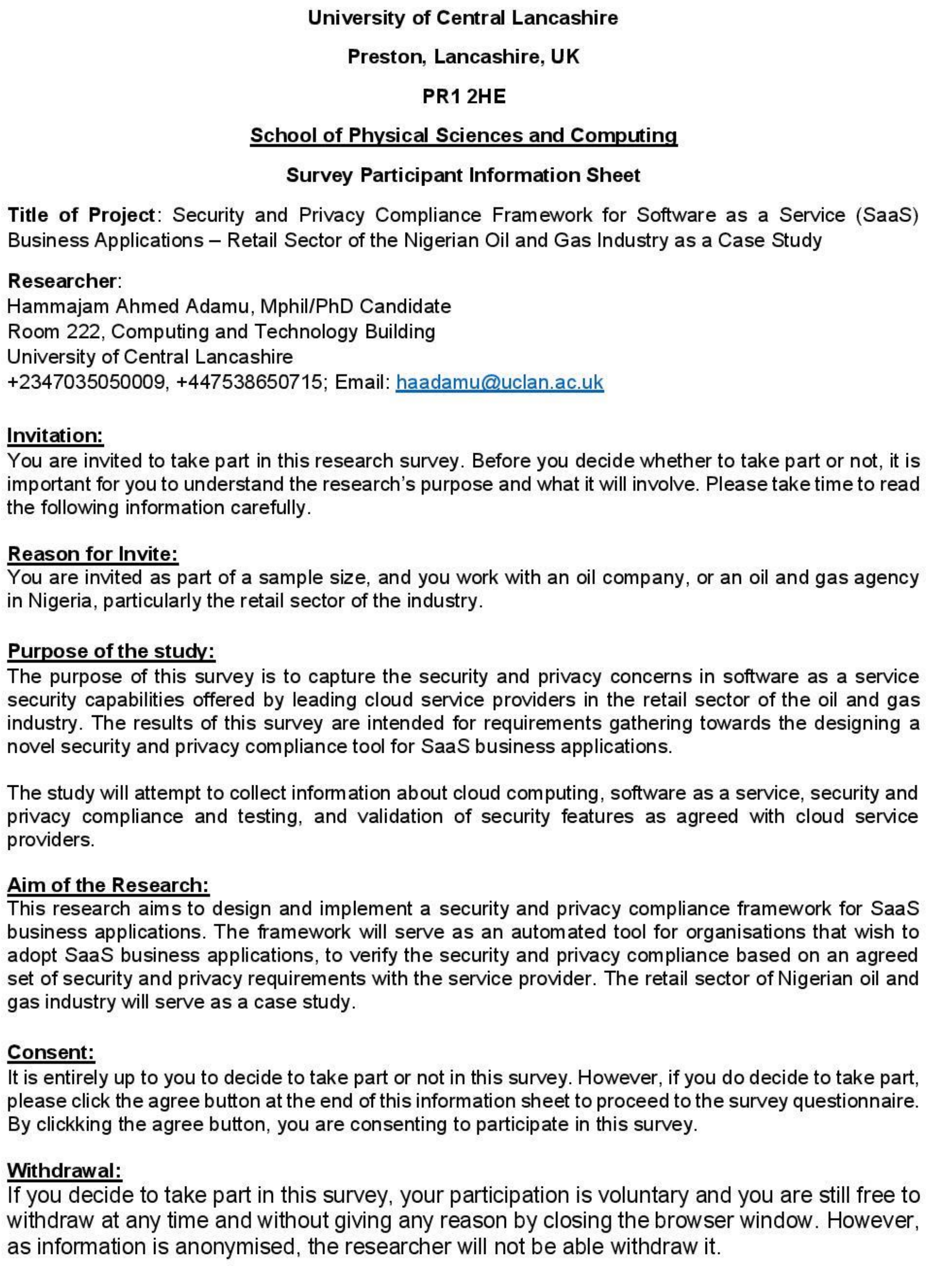
Yours sincerely

Julie Cook
Deputy Vice-Chair
STEMH Ethics Committee

* for research degree students this will be the final lapse date

NB - Ethical approval is contingent on any health and safety checklists having been completed and necessary approvals gained as a result.

Appendix 3: Questionnaire PIS



University of Central Lancashire

Preston, Lancashire, UK

PR1 2HE

School of Physical Sciences and Computing

Survey Participant Information Sheet

Title of Project: Security and Privacy Compliance Framework for Software as a Service (SaaS) Business Applications – Retail Sector of the Nigerian Oil and Gas Industry as a Case Study

Researcher:
Hammajam Ahmed Adamu, Mphil/PhD Candidate
Room 222, Computing and Technology Building
University of Central Lancashire
+2347035050009, +447538650715; Email: haadamu@uclan.ac.uk

Invitation:
You are invited to take part in this research survey. Before you decide whether to take part or not, it is important for you to understand the research's purpose and what it will involve. Please take time to read the following information carefully.

Reason for Invite:
You are invited as part of a sample size, and you work with an oil company, or an oil and gas agency in Nigeria, particularly the retail sector of the industry.

Purpose of the study:
The purpose of this survey is to capture the security and privacy concerns in software as a service security capabilities offered by leading cloud service providers in the retail sector of the oil and gas industry. The results of this survey are intended for requirements gathering towards the designing a novel security and privacy compliance tool for SaaS business applications.

The study will attempt to collect information about cloud computing, software as a service, security and privacy compliance and testing, and validation of security features as agreed with cloud service providers.

Aim of the Research:
This research aims to design and implement a security and privacy compliance framework for SaaS business applications. The framework will serve as an automated tool for organisations that wish to adopt SaaS business applications, to verify the security and privacy compliance based on an agreed set of security and privacy requirements with the service provider. The retail sector of Nigerian oil and gas industry will serve as a case study.

Consent:
It is entirely up to you to decide to take part or not in this survey. However, if you do decide to take part, please click the agree button at the end of this information sheet to proceed to the survey questionnaire. By clickking the agree button, you are consenting to participate in this survey.

Withdrawal:
If you decide to take part in this survey, your participation is voluntary and you are still free to withdraw at any time and without giving any reason by closing the browser window. However, as information is anonymised, the researcher will not be able withdraw it.

Procedure for Taking the Survey:

The Questionnaire consists of 45 questions in **five sections** namely:

i. Cloud Computing and Software-as-a-Service Assessment Section.
ii. SaaS Security and Privacy Assessment.
iii. SaaS Application Security and Privacy Compliance.
iv. Testing and Validation.
v. Demography.

The Questionnaire will take approximately 15-20 minutes or less to complete. The researcher formulated the questions to find out the concerns of security and privacy in cloud computing, and particularly in SaaS applications.

Microsoft forms survey tool will be used for data collection as Microsoft forms is a secure survey platform that is compliant with the new European Union General Data Protection Regulation of the European Union (EU-GDPR).

Responses will be required on some critical questions, which are identified by an asterisk sign *, and not all items.
You have up to 14 days to start and complete the survey. Once you start, you have 48hours to complete the survey.

IP Address:
The researcher will not keep records of the IP Addresses of the devices used by participants. The survey data will be removed at the expiration of the 14days from the survey platform and the data transferred to the Uclan network.

Selection Criteria
You have been selected as part of a sample size because you work with an oil company, or an oil and gas agency in Nigeria, particularly the retail sector. Additionally, you have been selected based on your role as Operations, IT, and Management Level Staff of your organisation.

Ethical Considerations, rights and regulations:

- You do not have to take part in this survey, as participation is voluntary.
- You can withdraw by simply closing the browser before completing the survey.
- The researcher will keep the data gathered through the questionnaire anonymised, confidential and will be used by the researcher and people with legitimate professional need.

The following legislation and guiding principles were considered in by this research study:

- The United Kingdom Data Protection Legislation 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted; https://www.eugdpr.org/the-regulation.html and
- The University of Central Lancashire's Ethical Principles for Teaching, Research, Consultancy, Knowledge Transfer & Related Activities (https://www.uclan.ac.uk/students/assets/files/Research_ethical_principles_Sept2015.pdf).

Benefits
There are no direct benefits for participants. However, the researcher hopes that through your participation, we will learn more about security and privacy concerns of the oil and gas industry adopting SaaS applications in their operations especially, the retail sector.

The researcher may earn academic credit, at the discretion of his supervisory team towards the award of an MPhil/PhD with the University of Central Lancashire, United Kingdom.

Risks
The researcher does not anticipate any risk or harm to come upon any participant in this for taking this survey.

Confidentiality
All information obtained from participants by the researcher will be stored securely on the University Cloud Platform.

The University's policy on Academic Integrity will govern the retention of data generated by this study. The researcher will keep securely the Data generated in paper or electronic form for five years to the end of the project.

Results of the research study
The results of the outcome of this research will be part of the final thesis of the researcher leading to the award of a PhD Degree.

The findings of the survey will be available online after 31/12/2018 in the Petroleum Technology development Fund peer-reviewed journal and other academic journals where electronic copies will be available for download.

Funding of Research
The Researcher is a student at the University of Central Lancashire with the Department of Computing, School of Physical Sciences and Computing.

The Federal Government of Nigeria through the Petroleum Technology Development Fund funds this research.

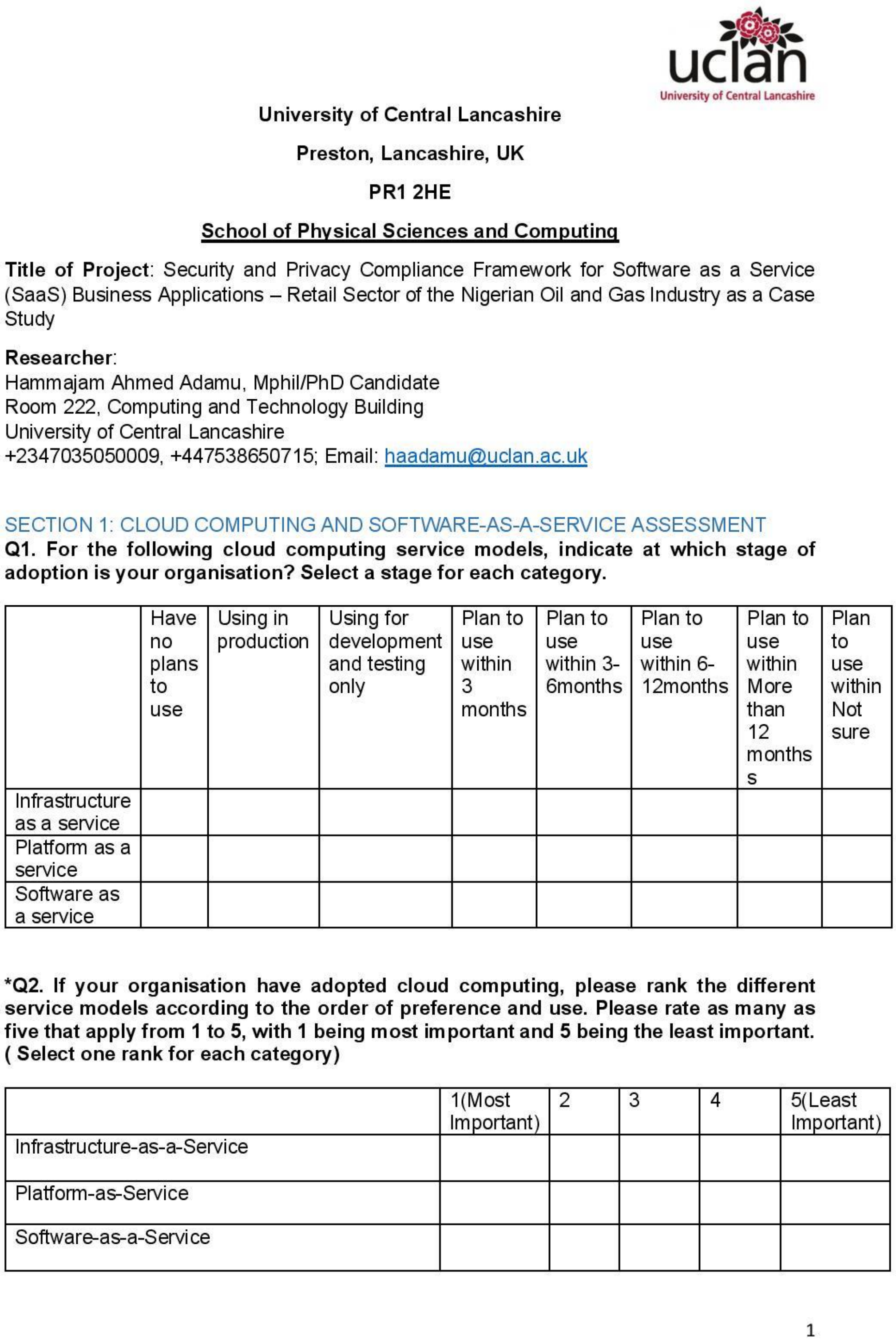
Review and Approval
This research work has been reviewed and approved by the University Research Ethics Committee (Science, Technology, Engineering, Medicine and Health STEMH)

Contact for Further Information
Please contact any member of our team as listed below.

Hammajam Ahmed Adamu Mphil/PhD Candidate, Room CM222, haadamu@uclan.ac.uk Computing and Technology Building University of Central Lancashire, United Kingdom +447538650715	**Dr Max Eiza** Director of Studies (Supervisor I), Room CM213, mhashemeiza@uclan.ac.uk Computing and Technology Building University of Central Lancashire, United Kingdom +441772893169	**Dr Vinh Thong Ta** Supervisor II, Room CM116 vtta@uclan.ac.uk Computing and Technology Building University of Central Lancashire United Kingdom +441772 89 3263

If you have any concerns about the way in which the study has been conducted, you should contact University Officer for Ethics (email address: OfficerforEthics@uclan.ac.uk).

Appendix 4: Questionnaire Survey Questions



University of Central Lancashire

Preston, Lancashire, UK

PR1 2HE

School of Physical Sciences and Computing

Title of Project: Security and Privacy Compliance Framework for Software as a Service (SaaS) Business Applications – Retail Sector of the Nigerian Oil and Gas Industry as a Case Study

Researcher:
Hammajam Ahmed Adamu, Mphil/PhD Candidate
Room 222, Computing and Technology Building
University of Central Lancashire
+2347035050009, +447538650715; Email: haadamu@uclan.ac.uk

SECTION 1: CLOUD COMPUTING AND SOFTWARE-AS-A-SERVICE ASSESSMENT

Q1. For the following cloud computing service models, indicate at which stage of adoption is your organisation? Select a stage for each category.

	Have no plans to use	Using in production	Using for development and testing only	Plan to use within 3 months	Plan to use within 3-6months	Plan to use within 6-12months	Plan to use within More than 12 months s	Plan to use within Not sure
Infrastructure as a service								
Platform as a service								
Software as a service								

***Q2. If your organisation have adopted cloud computing, please rank the different service models according to the order of preference and use. Please rate as many as five that apply from 1 to 5, with 1 being most important and 5 being the least important. (Select one rank for each category)**

	1(Most Important)	2	3	4	5(Least Important)
Infrastructure-as-a-Service					
Platform-as-Service					
Software-as-a-Service					

***Q3. What does your organisation view as the most important benefits of cloud computing? Of the factors and drivers below, please rank as many as five, with 1 as the most important and 5 as the least important. (Select one rank for each factor)**

	1(Most Important)	2	3	4	5(Least Important)
Cost savings on hardware					
Cost savings on software					
Cost savings on IT operations staff					
Ability to launch new products and services					
Ability to grow and shrink IT capacity on demand					
Convenience for the development teams					
No upfront investment					
Pricing flexibility					
Better collaboration across teams					
Outsourcing of non-core competencies					

Other (please specify and rank)

***Q4. What are the most significant barriers to adoption of software as a service in your organisation? Please rank the five most important factors or concerns below, with 1 as the most important and 5 as the least important.**

	1(Most Important)	2	3	4	5(Least Important)
Reliability					
Interoperability challenges					
Performance					
Geographic Location of Cloud Provider Data Centers					
Security					
Compliance					
Lack of Ability to Customize					
Integration with Existing Systems					
Costs and Return On Investment					
Lack of Management Understanding / Willing to Innovate					
Not sure					
We did not have any concerns					

Other (please specify and rank)

The researcher is interested in understanding the process by which organisations adopt software as a service. For the next three questions, please consider the following statement: *If your organisation is already using or planning to use Software-as-a-service model, how did the process unfold?*

Q5. Who initiated the adoption of Software as a service in your organisation?

An IT operations team □

A departmental Project □

A CEO decision □

A CIO/Senior IT Exec Decision □

Not Sure □

Others (Please specify)

***Q6. For which types of applications or areas of operations do you use the software as a service? Please check all that apply:**

Internal Enterprise (Payroll, Enterprise Resource Planning) □

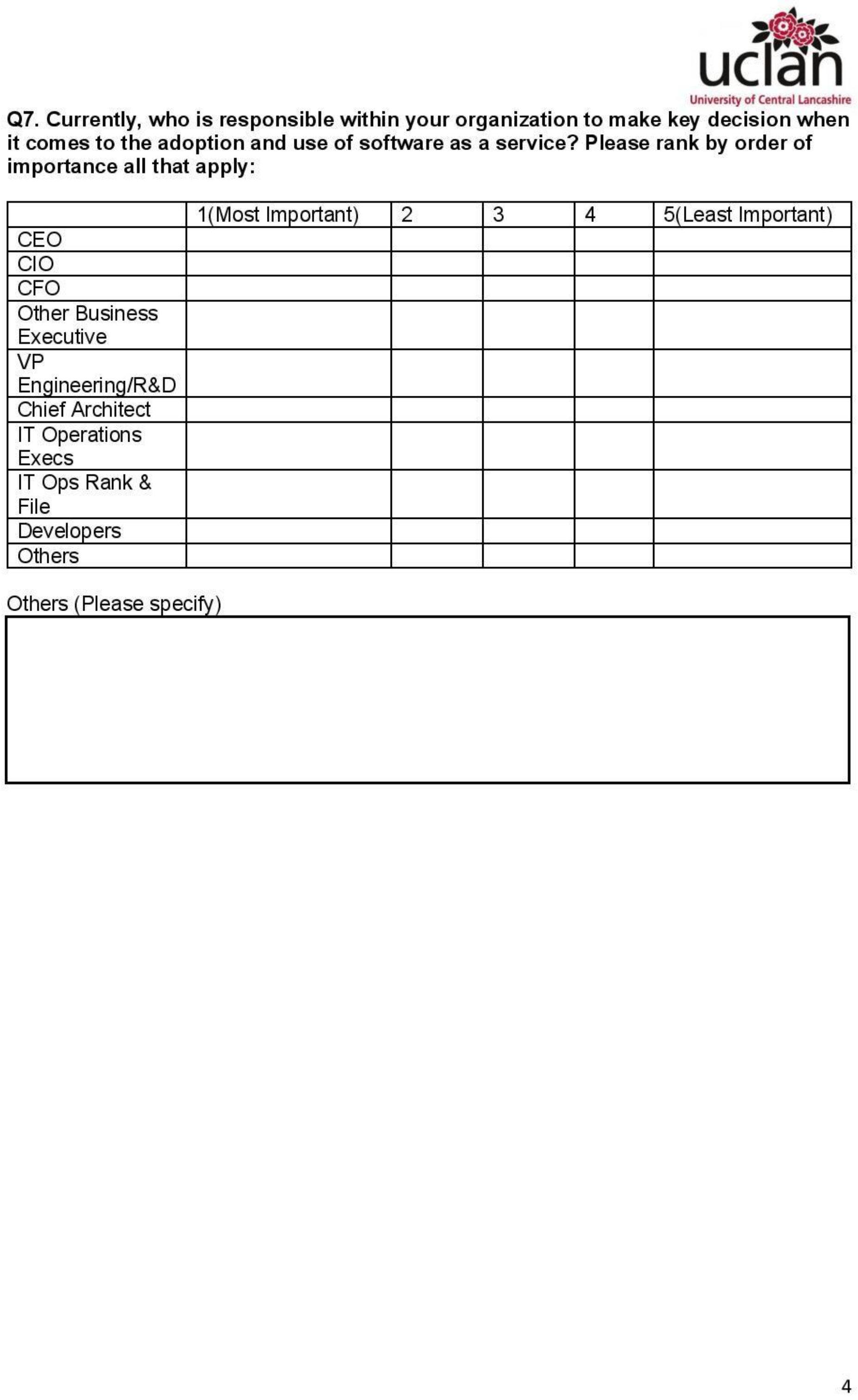
Office Productivity □

Customer Relationship Management □

Operations □

Marketing/Business intelligence □

Others □



Q7. Currently, who is responsible within your organization to make key decision when it comes to the adoption and use of software as a service? Please rank by order of importance all that apply:

	1(Most Important)	2	3	4	5(Least Important)
CEO					
CIO					
CFO					
Other Business Executive					
VP Engineering/R&D					
Chief Architect					
IT Operations Execs					
IT Ops Rank & File					
Developers					
Others					

Others (Please specify)

***Q8. If your organisation is using Software-as-a-service, how much does your organisation plan to spend per month on the following Service models within the next 12 months?**
(Drop down list)

	Hardware/Network/Storage	Software
Software as a Service	Not using this solution Less than $1000 per month $1000-$5000 per month $5000-$10000 per month More than $10000 per month	Not using this solution Less than $1000 per month $1000-$5000 per month $5000-$10000 per month More than $10000 per month
Infrastructure-as-a-Service	Not using this solution Less than $1000 per month $1000-$5000 per month $5000-$10000 per month More than $10000 per month	Not using this solution Less than $1000 per month $1000-$5000 per month $5000-$10000 per month More than $10000 per month
Platform-as-a-Service	Not using this solution Less than $1000 per month $1000-$5000 per month $5000-$10000 per month More than $10000 per month	Not using this solution Less than $1000 per month $1000-$5000 per month $5000-$10000 per month More than $10000 per month

Q9. How many employees work at your organisation?

Less than 100	
100-500	
501-1000	
1001-5000	
5001-10000	
More than 10000	

Q10. Is there any additional information you will like to say about the adoption or use of Software as a Service in your organisation?

SECTION 2: SAAS SECURITY AND PRIVACY ASSESSMENT SECTION

AUTHENTICATION

***Q11.Which authentication solution would you prefer for your software-as-a-service applications?**

SaaS Service provider authentication □

Organisation's authentication system/solution (AD, LDAP) □

Third party cloud-based authentication (SSO, Shiloh, and Gatekeeper) □

I do not know □

Other (Please, Specify) □

Q12. Do you have guarantees for passwords encryption for data in transit?

Yes □

No □

Not Sure □

Others □

Please explain briefly.

Q13. Are passwords encrypted in storage?

Yes □

No □

Not Sure □

Please explain briefly.

AUTHORIZATION- Access Control

Q14. Does your platform directory service authorise users?

Yes □

No □

Not Sure □

Please explain briefly

Q15. If YES, which solution?

LDAP □

On-Premise AD □

Azure Cloud AD □

Single-Sign-On (third party authorisation solution) □

Not Sure □

***Q16. Are users authorised by the SaaS Service Provider's system?**

Yes □

No □

Not Sure □

Please explain briefly

DATA SECURITY AND PRIVACY

***Q17. Is there an evidence from your SaaS service provider that all network transfer of your Data is encrypted when traversing the Service provider's network?**

Yes □

None □

Not Sure □

Others □

Please explain briefly

***Q18. Does your SaaS service provider implement appropriate controls to ensure data integrity (e.g. input validation, transaction redo logs)?**

Yes □

No □

Do Not Know □

Other (Please specify) □

Please explain briefly

Q19. Do you have a mechanism for logging user-level access for monitoring purposes? If YES,
Can this collected log data be made available to your organisation by your SaaS provider?

Yes □

No □

Do Not Know □

Other (Please specify) □

DATA RECOVERY (BACKUP)

Q20. Does your organisation have a clear recoverability objective agreed with the SaaS service provider?

Yes □

No □

Do Not Know □

Other (Please specify) □

Q21. Does your organisation's SaaS service provider have a data and system backup plan aligned with your organisation's recoverability objective?

Yes □

No □

Do Not Know □

Other (Please specify □

OPERATIONAL CONTROLS

Q22. Does your organisation's SaaS service provider provide you with information regarding where the software application resides?

Yes □

No □

Do Not Know □

Others □

(Please specify)

***Q23. Is your SaaS service provider hosting their application on their own data storage location or a third party?**

Yes □

No □

Do Not Know □

Q24. Has your SaaS service provider gave your organisation an evidence of measures to ensure the physical security of the data centre (s) where the application and data storage servers are warehoused?

Yes □

No □

Do Not Know □

Other (Please specify) □

***Q25. If your service provider is currently providing the same service to other clients, is multi-tenant access effectively controlled to ensure users access only the data they are authorised to access?**

Yes □

No □

Don’t Know □

Other (Please specify) □

***Q26. Does the service provider maintain and apply host security standards on their servers and verify them whenever new changes introduced into the system?**

Yes □

No □

Do Not Know □

Other (Please specify) □

INCIDENCE RESPONSE

***Q27. Does your service provider have a documented process for reporting security incidents involving systems used to store/access/modify hosted data to your IT contact?**

Yes □

No □

Do Not Know □

Other (Please specify) □

Q28. Do data hosting customers share incident information and common vulnerabilities or threats?

Yes □

No □

Do Not Know □

Other (Please specify)

□

SECTION 3: SOFTWARE-AS-A-SERVICE APPLICATION SECURITY

***Q30. Does the software development life-cycle model used by your SaaS service provider in the development of their software, incorporate specific controls from any standards-based framework models? Please select appropriate framework.**

Cloud Security Alliance □

Cloud Control Matrix □

OWASP □

NIST SP800-64 rev v2 □

ISO 27001/27002 □

I do not know □

If other, please specify.

Q31. Are security controls of components identified and represented during each phase of the software development lifecycle?

Yes □

No □

Do Not Know □

Other (Please specify) □

Q32. Does your SaaS service provider have a change management policy in place to guide the introduction of new features to your SaaS application?

Yes □

No □

Do Not Know □

Other (Please specify) □

Q32.Is the SaaS service provider's application restricted to encrypted channels (e.g. https)?

Yes □

No □

Do Not Know □

Other (Please specify) □

SECTION 4: SECURITY AND PRIVACY COMPLIANCE SECTION

***Q33. How do you verify Security and Privacy Compliance in your Software-as-a-Service subscription as provided by your Service Provider?**

Assurances from Service Provider □

Manual auditing □

Logs □

Automated compliance tool □

Other (Please specify) □

***Q34. Are risk assessments performed on a regular basis or whenever the system, facilities, or other conditions change?**

Yes, risk assessments are performed on our systems regularly. □

No, no risk assessments are not performed on our systems regularly. □

I Do not Know □

***Q35. Can your SaaS application service provider make available a test evaluation instance of the SaaS application?**

Yes □

No □

I do not know □

Others (Please specify □

***Q36. If yes, can the test instance be used by your IT security staff to VALIDATE security and privacy compliance?**

Yes □

No □

I do not know □

Others (Please specify □

***Q37. Do you agree that it is necessary to have an automated tool to help you verify the security and privacy compliance of your Software-as-a-service business application?**

Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
○	○	○	○	○

***Q38. Can your Software-as-a-service Test evaluation instance include access to both the user-level interface and Application Programming Interface or engine?**

Yes □

No □

Do not know □

Others □

(Please, specify)

***Q39. If, yes, do you agree with the statement that automated security and privacy tool will help your organisation in ensuring the integrity and security of data with your software as a service application provider?**

Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
○	○	○	○	○

SECTION 5: DEMOGRAPHY

Q40. What is your job rank?

Senior management	□
Middle management	□
Operations Manager	□
Middle management	□
IT-Technical Staff	□
Operations Manager	□
IT Support	□

Other ____________________
(Please, specify)

Q41. My department unit is:

Information Technology □

Security and Compliance □

Information System □

Finance □

Human resource management □

Customer Service □

General Administration □

Other ____________________ □

Q42. How long have you been working in your organisation?

Less than 5 years □

5-10 Years □

10 or more Years □

Other □

(Please, specify)

Q43. Gender

Male □

Female □

Prefer not to say □

Q44. Age Group

30 and under □

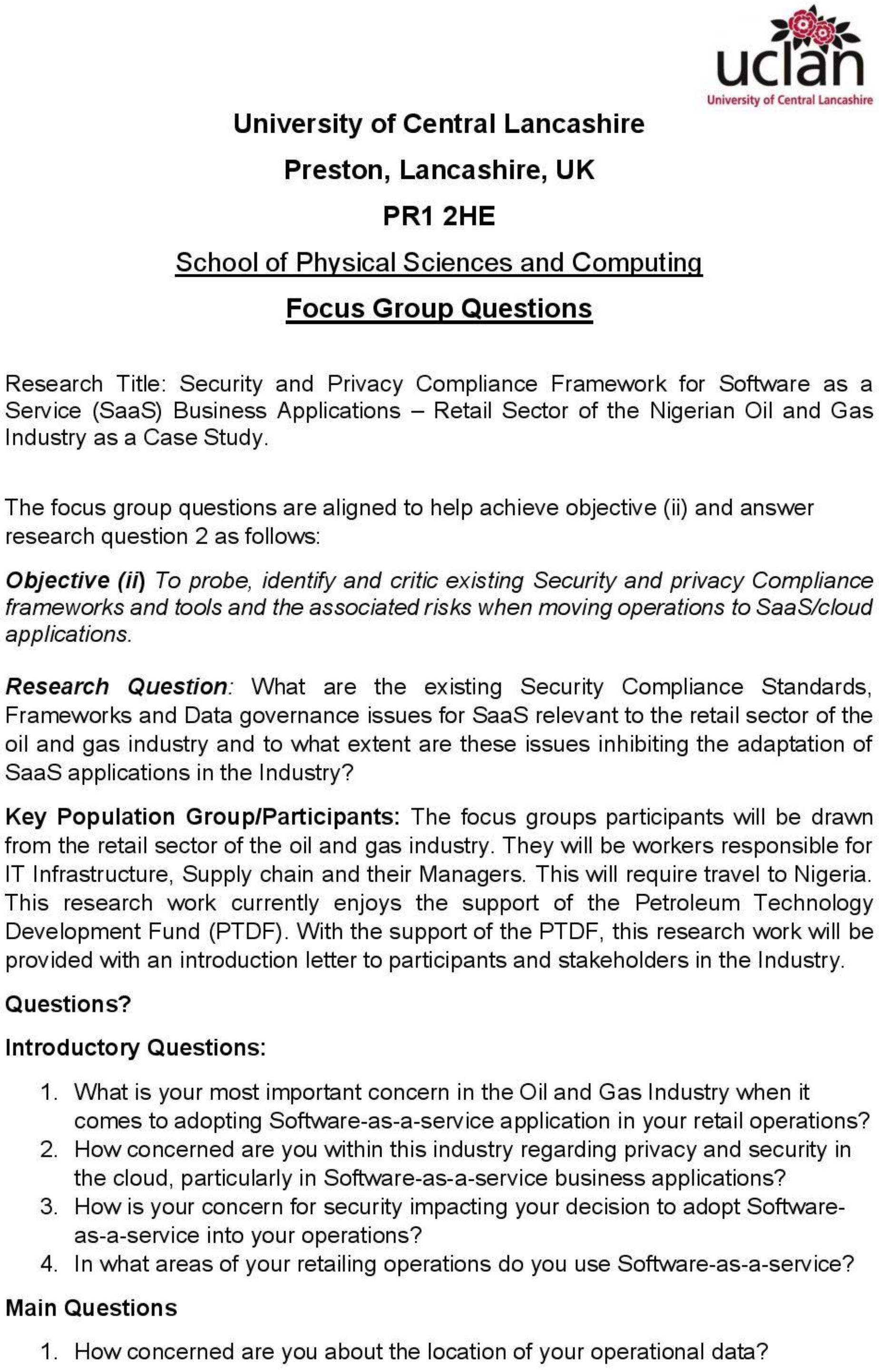
31-40 □

41-50 □

50+ □

Prefer not to say □

Appendix 5: Focus Group Questions



University of Central Lancashire

Preston, Lancashire, UK

PR1 2HE

School of Physical Sciences and Computing

Focus Group Questions

Research Title: Security and Privacy Compliance Framework for Software as a Service (SaaS) Business Applications – Retail Sector of the Nigerian Oil and Gas Industry as a Case Study.

The focus group questions are aligned to help achieve objective (ii) and answer research question 2 as follows:

Objective (ii) *To probe, identify and critic existing Security and privacy Compliance frameworks and tools and the associated risks when moving operations to SaaS/cloud applications.*

***Research Question**:* What are the existing Security Compliance Standards, Frameworks and Data governance issues for SaaS relevant to the retail sector of the oil and gas industry and to what extent are these issues inhibiting the adaptation of SaaS applications in the Industry?

Key Population Group/Participants: The focus groups participants will be drawn from the retail sector of the oil and gas industry. They will be workers responsible for IT Infrastructure, Supply chain and their Managers. This will require travel to Nigeria. This research work currently enjoys the support of the Petroleum Technology Development Fund (PTDF). With the support of the PTDF, this research work will be provided with an introduction letter to participants and stakeholders in the Industry.

Questions?

Introductory Questions:

1. What is your most important concern in the Oil and Gas Industry when it comes to adopting Software-as-a-service application in your retail operations?
2. How concerned are you within this industry regarding privacy and security in the cloud, particularly in Software-as-a-service business applications?
3. How is your concern for security impacting your decision to adopt Software-as-a-service into your operations?
4. In what areas of your retailing operations do you use Software-as-a-service?

Main Questions

1. How concerned are you about the location of your operational data?

2. What technical enforcement mechanisms does your cloud service provider use to prevent access to your data by other users residing on the same hardware due to multi-tenancy?
3. What established frameworks does your cloud service provider use for the enforcement of security and privacy controls?
4. How do you ensure compliance with those frameworks and standards?
5. Does your cloud service provider ensure compliance with third-party audits or an automated tool?

Closing Questions:

1. Can you as a customer audit the Cloud Service Provider's in-house security controls?
2. Can automation of some specific controls from standard security frameworks help improve the security of your data?
3. Will you move all your business applications into the cloud if you can verify compliance using an automated tool?
4. Are their other concerns apart from security and privacy issues that are hindering your migration to the cloud and using software-as-a-service?

Guidelines/Considerations

Number of Participants: 6

Environment: Comfortable, Circle seating and Audio Recorded.

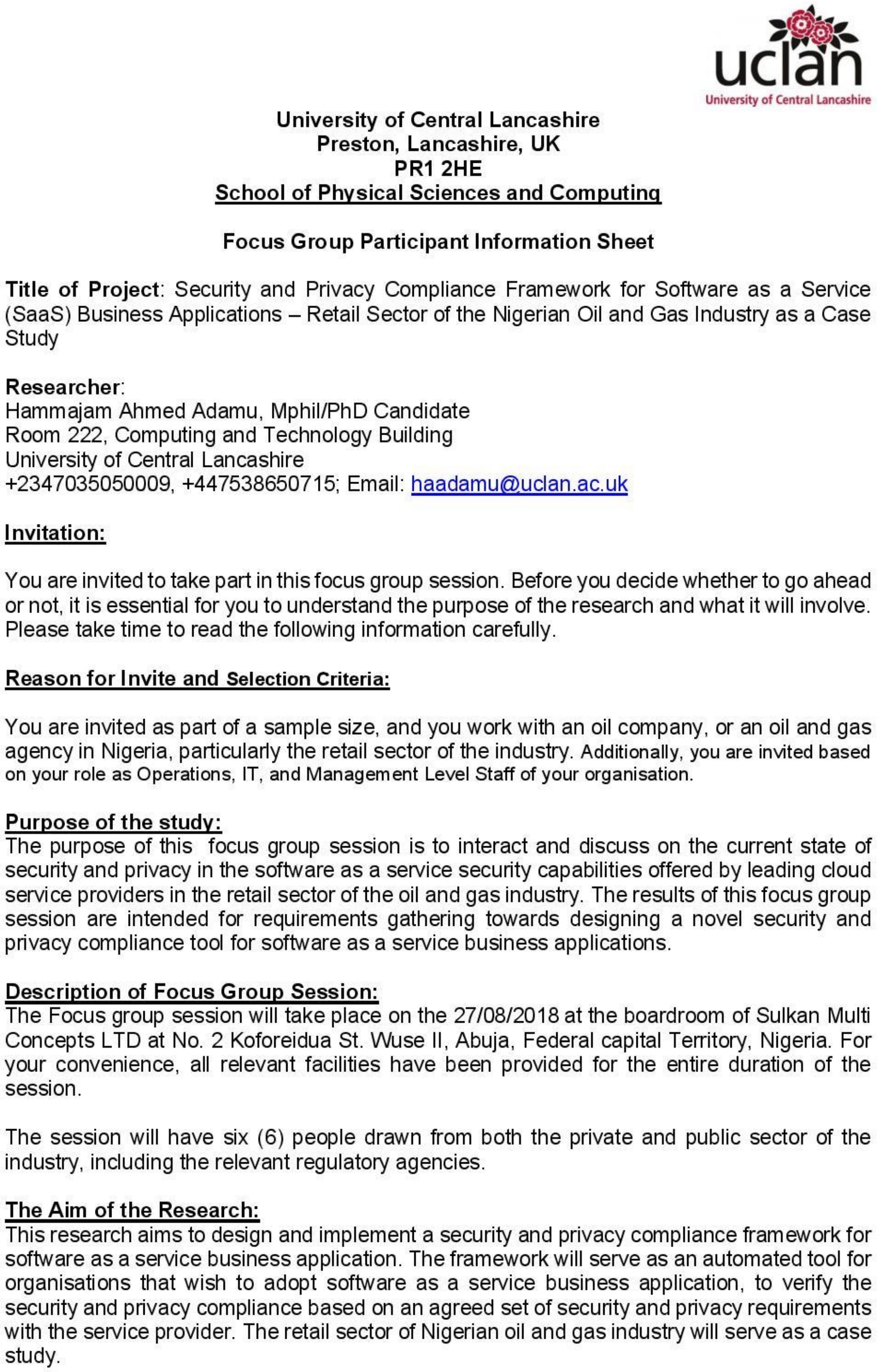
Moderator: A Moderator will moderate the discussion. (The researcher will take on this responsibility)

Assistant Moderator: An assistant moderator will be engaged to handle logistics and take notes. The assistant will also setup venue and assist participants to settle in the venue.

Analysis and Reporting: Appropriate Reporting will be prepared by the researcher in addition to the data collected using the questionnaire.

Permission: Will be sought to record in audio of the entire session. Consent forms will be administered.

Appendix 6: Focus Group PIS



University of Central Lancashire
Preston, Lancashire, UK
PR1 2HE
School of Physical Sciences and Computing

Focus Group Participant Information Sheet

Title of Project: Security and Privacy Compliance Framework for Software as a Service (SaaS) Business Applications – Retail Sector of the Nigerian Oil and Gas Industry as a Case Study

Researcher:
Hammajam Ahmed Adamu, Mphil/PhD Candidate
Room 222, Computing and Technology Building
University of Central Lancashire
+2347035050009, +447538650715; Email: haadamu@uclan.ac.uk

Invitation:

You are invited to take part in this focus group session. Before you decide whether to go ahead or not, it is essential for you to understand the purpose of the research and what it will involve. Please take time to read the following information carefully.

Reason for Invite and Selection Criteria:

You are invited as part of a sample size, and you work with an oil company, or an oil and gas agency in Nigeria, particularly the retail sector of the industry. Additionally, you are invited based on your role as Operations, IT, and Management Level Staff of your organisation.

Purpose of the study:
The purpose of this focus group session is to interact and discuss on the current state of security and privacy in the software as a service security capabilities offered by leading cloud service providers in the retail sector of the oil and gas industry. The results of this focus group session are intended for requirements gathering towards designing a novel security and privacy compliance tool for software as a service business applications.

Description of Focus Group Session:
The Focus group session will take place on the 27/08/2018 at the boardroom of Sulkan Multi Concepts LTD at No. 2 Koforeidua St. Wuse II, Abuja, Federal capital Territory, Nigeria. For your convenience, all relevant facilities have been provided for the entire duration of the session.

The session will have six (6) people drawn from both the private and public sector of the industry, including the relevant regulatory agencies.

The Aim of the Research:
This research aims to design and implement a security and privacy compliance framework for software as a service business application. The framework will serve as an automated tool for organisations that wish to adopt software as a service business application, to verify the security and privacy compliance based on an agreed set of security and privacy requirements with the service provider. The retail sector of Nigerian oil and gas industry will serve as a case study.

Consent
It is up to you to decide whether to take part or not in this focus group session. However, if you do choose to take part, you will be given this participant information sheet to keep, and you will be asked to sign a consent form.

Withdrawal:
If you decide to take part in this focus group, your participation is voluntary and you are still free to withdraw at any time and without giving any reason.

However, it will not be possible to withdraw participant data from the study after final analysis has been undertaken.

Procedure for Taking Part in the Focus Group Session

The entire duration of the session will only last approximately 45 minutes to 1 hour, and themes and questions will focus on Software as a Service, Security and Privacy Compliance and issues bothering on ensuring compliance by service providers.

Recording Focus Group Session
The Researcher will audio record the entire session session. However, if you do not wish to be recorded, then you will not be able to participate in this session.

Refreshments and Light Meal
The researcher has arranged for light snacks and meal for your convenience while the session lasts.

Benefits
There are no direct benefits for participants. However, it is hoped that through your participation, we will learn more about security and privacy concerns of the oil and gas industry especially, the retail sector.

The researcher may earn academic credit, at the discretion of his supervisory team towards the award of an MPhil/PhD with the University of Central Lancashire, United Kingdom.

Risks
The researcher does not anticipate any risk or harm to come upon any participant in this focus group session.

Confidentiality
All information obtained from participants by the researcher will be stored securely on the University Cloud Platform.

The University's policy on Academic Integrity will govern the retention of data generated by this study. The researcher will keep securely the Data generated in paper or electronic form for five years to the end of the project.

Participation/Opt-In
By signing the consent form, you are saying that you have read this information and therefore, understand what you are being asked to do and you are, therefore, consenting to opt-in and participate in this focus group session.

Results of the research study

The results of the outcome of this research will be part of the final thesis of the researcher leading to the award of a PhD Degree.

The findings of the study will be available online after 31/12/2018 in the Petroleum Technology development fund peer-reviewed journal and other academic journals where electronic copies will be available for download.

Funding of Research

The Researcher is a Student at the University of Central Lancashire with the Department of Computing, School of Physical Sciences and Computing.
The Federal Government of Nigeria through the Petroleum Technology Development Fund funds this research.

Review and Approval

This research work has been reviewed and approved by the University Research Ethics Committee (Science, Technology, Engineering, Medicine and Health STEMH)

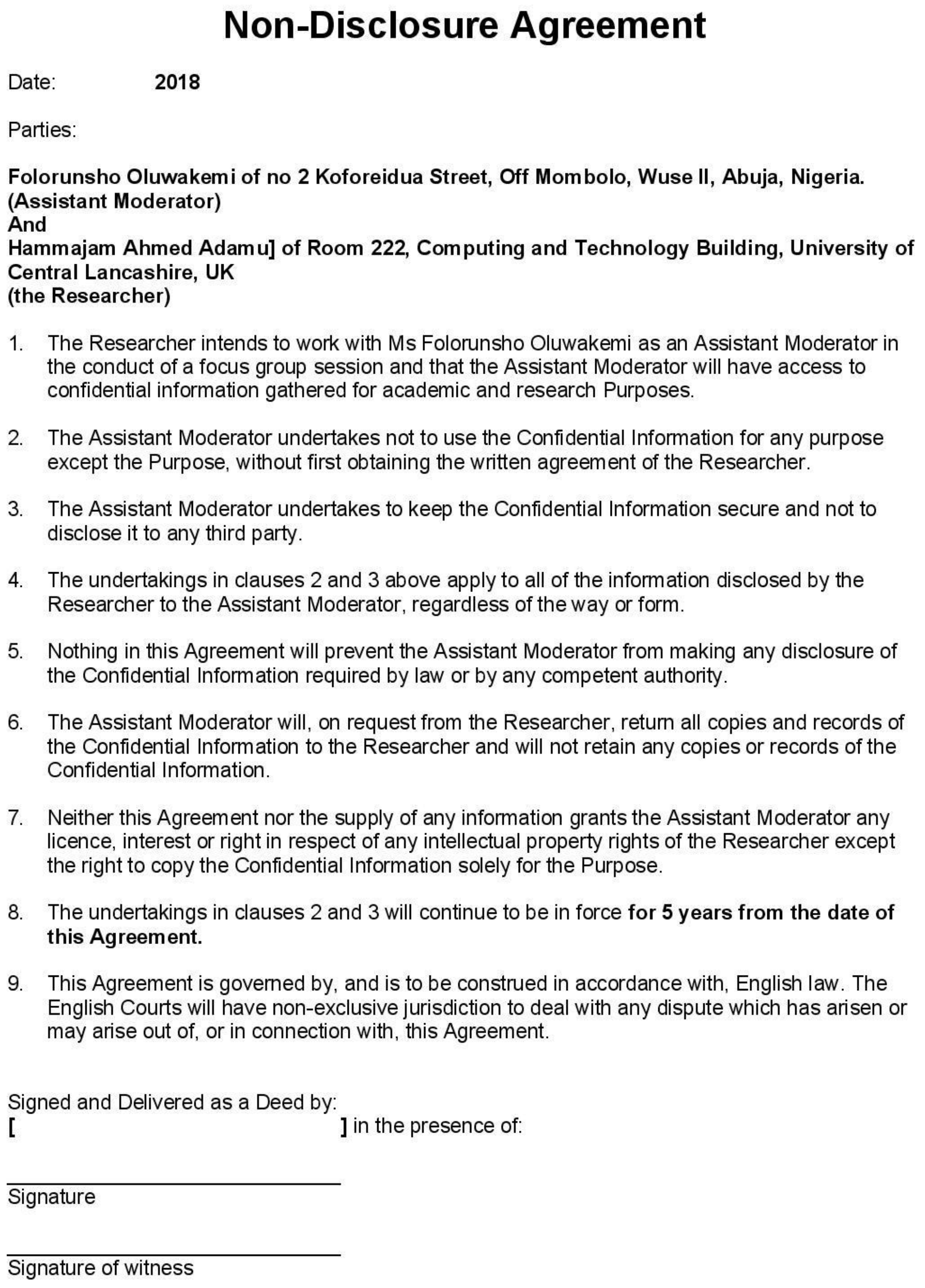
Contact for Further Information

Please contact any member of our team as listed below.

Hammajam Ahmed Adamu	**Dr Max Eiza**	**Dr Vinh Thong Ta**
Mphil/PhD Candidate, Room CM222, haadamu@uclan.ac.uk Computing and Technology Building University of Central Lancashire, United Kingdom +447538650715	Director of Studies (Supervisor I), Room CM213, mhashemeiza@uclan.ac.uk Computing and Technology Building University of Central Lancashire, United Kingdom +441772893169	Supervisor II, Room CM116 vtta@uclan.ac.uk Computing and Technology Building University of Central Lancashire United Kingdom +441772 89 3263

If you have any concerns about the way in which the study has been conducted, you should contact University Officer for Ethics (email address: OfficerforEthics@uclan.ac.uk).

Appendix 7: Non-Disclosure Agreement- Focus Group



Non-Disclosure Agreement

Date: **2018**

Parties:

Folorunsho Oluwakemi of no 2 Koforeidua Street, Off Mombolo, Wuse II, Abuja, Nigeria.
(Assistant Moderator)
And
Hammajam Ahmed Adamu] of Room 222, Computing and Technology Building, University of Central Lancashire, UK
(the Researcher)

1. The Researcher intends to work with Ms Folorunsho Oluwakemi as an Assistant Moderator in the conduct of a focus group session and that the Assistant Moderator will have access to confidential information gathered for academic and research Purposes.

2. The Assistant Moderator undertakes not to use the Confidential Information for any purpose except the Purpose, without first obtaining the written agreement of the Researcher.

3. The Assistant Moderator undertakes to keep the Confidential Information secure and not to disclose it to any third party.

4. The undertakings in clauses 2 and 3 above apply to all of the information disclosed by the Researcher to the Assistant Moderator, regardless of the way or form.

5. Nothing in this Agreement will prevent the Assistant Moderator from making any disclosure of the Confidential Information required by law or by any competent authority.

6. The Assistant Moderator will, on request from the Researcher, return all copies and records of the Confidential Information to the Researcher and will not retain any copies or records of the Confidential Information.

7. Neither this Agreement nor the supply of any information grants the Assistant Moderator any licence, interest or right in respect of any intellectual property rights of the Researcher except the right to copy the Confidential Information solely for the Purpose.

8. The undertakings in clauses 2 and 3 will continue to be in force **for 5 years from the date of this Agreement.**

9. This Agreement is governed by, and is to be construed in accordance with, English law. The English Courts will have non-exclusive jurisdiction to deal with any dispute which has arisen or may arise out of, or in connection with, this Agreement.

Signed and Delivered as a Deed by:
[ ] in the presence of:

____
Signature

____
Signature of witness

____
Name of witness

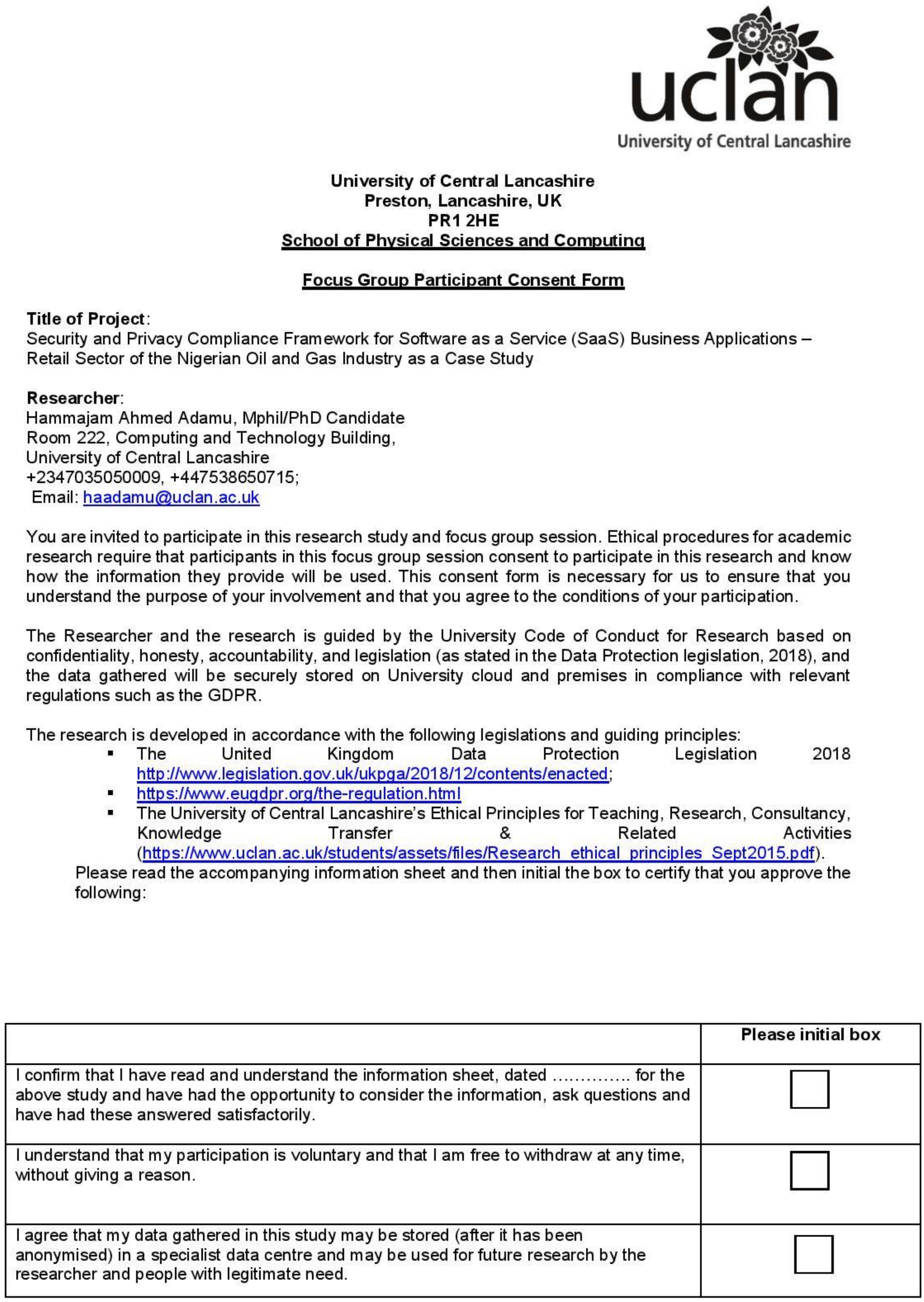
____

____

____

Address of witness

Appendix 8: Focus Group Consent Form



University of Central Lancashire
Preston, Lancashire, UK
PR1 2HE
School of Physical Sciences and Computing

Focus Group Participant Consent Form

Title of Project:
Security and Privacy Compliance Framework for Software as a Service (SaaS) Business Applications – Retail Sector of the Nigerian Oil and Gas Industry as a Case Study

Researcher:
Hammajam Ahmed Adamu, Mphil/PhD Candidate
Room 222, Computing and Technology Building,
University of Central Lancashire
+2347035050009, +447538650715;
Email: haadamu@uclan.ac.uk

You are invited to participate in this research study and focus group session. Ethical procedures for academic research require that participants in this focus group session consent to participate in this research and know how the information they provide will be used. This consent form is necessary for us to ensure that you understand the purpose of your involvement and that you agree to the conditions of your participation.

The Researcher and the research is guided by the University Code of Conduct for Research based on confidentiality, honesty, accountability, and legislation (as stated in the Data Protection legislation, 2018), and the data gathered will be securely stored on University cloud and premises in compliance with relevant regulations such as the GDPR.

The research is developed in accordance with the following legislations and guiding principles:

- The United Kingdom Data Protection Legislation 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted;
- https://www.eugdpr.org/the-regulation.html
- The University of Central Lancashire's Ethical Principles for Teaching, Research, Consultancy, Knowledge Transfer & Related Activities (https://www.uclan.ac.uk/students/assets/files/Research_ethical_principles_Sept2015.pdf).

Please read the accompanying information sheet and then initial the box to certify that you approve the following:

	Please initial box
I confirm that I have read and understand the information sheet, dated …………. for the above study and have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	□
I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason.	□
I agree that my data gathered in this study may be stored (after it has been anonymised) in a specialist data centre and may be used for future research by the researcher and people with legitimate need.	□

I understand that it will not be possible to withdraw my data from the audio recording and the study after final analysis has been undertaken	□
I agree to the interview / focus group / consultation being audio recorded	□
I agree to the use of anonymised quotes in publications	□
I agree to take part in the above focus group session.	□

Name of Participant Date Signature

Name of Researcher Date Signature

If you have any queries, please contact:
Hammajam Ahmed Adamu on telephone: +2347035050009, +447538650715; Email: haadamu@uclan.ac.uk
……
……………………………………..
The Researcher intends to provide feedback on the research from the data gathered from the questionnaire after 31/12/2018 in the Petroleum Technology development Fund peer-reviewed journal and other academic journals where electronic copies will be available for download.

Thank you.