An analysis of the potential impact of data protection and data security law reform to the position of employees in Indonesian cloud computing industry

Rama Kumala Sari

July, 2019.

This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy.

Postgraduate Studies (Research), Law School,
Lancaster University, UK.

An analysis of the potential impact of data protection and data security law reform to the position of employees in Indonesian cloud computing industry

Rama Kumala Sari

Word count – 71,003

This thesis results entirely from my own work and has not been offered previously for any degree or diploma.

Signature ……..

Abstract

Cloud computing has raised both technological and legal issues in its implementation. The readiness and the awareness of the legal effect of the implementation of cloud computing in the workplace should be distributed and applied among the employees, most importantly, the policy makers. They have a significant duty to create full legal awareness by making sure all the employees have complied with the regulations and policies.

This study sought to determine whether there was adequate support from the Information and communications technology (ICT) companies in Indonesia for their employees, related to their understanding of and readiness for the implementation of cloud computing, data security and data protection. This thesis analyses the extent to which the Indonesian cloud computing industry would be affected by wide-ranging data protection and data security law reforms, and to evaluate the potential effect that data protection and data security law reform could have on the position of employees in the sector.

This study uses empirical legal research to analyse the implications of the development of cloud computing, especially for data security and data protection frameworks in the ICT industry. It studies the relevant law and uses interviews to reveal up-to-date data and depict the real situation in the workplace. This thesis examine the regulation and policy in the European Union and United Kingdom, since they have developed a robust set of protections in data security and data protection. Classical content analysis is used to examine the transcripts from semi-structured interviews and data from legal documents and employment policies.

The findings of the research support the growth of ICT employees' skills and the growth of the cloud computing industry in Indonesia and highlight the implementation of legal aspects in ICT companies and the effect of the development of technology from the policy makers' perspective.

Acknowledgements

"I am with you and will watch over you wherever you go, and I will bring you back to this land. I will not leave you until I have done what I have promised you."
Genesis 28: 15

I would like to thank PT Telkom Indonesia, Tbk., for giving me the opportunity, support and funding through the scholarship which has encouraged me to do my best in pursuing my dream. I also want to express my sincere thanks to all the people in PT Telkom Indonesia, Tbk., who helped me to get through the research process, who from the beginning have trusted me and supported my research.

Most importantly, I would like to thank my supervisors, Dr Catherine Easton and Dr Mark Butler, who provided me with knowledge and guidance in the supervisory process. I feel blessed to have them as my supervisors. Thank you for your abundant patience during the research process. In addition, I would like to highlight their professionalism in communicating their knowledge and experiences in the fields of technology law and employment law.

I would like to extend my thanks to Lancaster University, the Student Based Services, the Administrator, the Librarian, and especially for the Postgraduate Studies (Research) Office, Law School, Lancaster University School of Law, for supporting me during my studies. There are several people who, for good reasons, deserve a place in this acknowledgement. I should thank the Revd Chris Newlands, Vicar of Lancaster, The Revd Dr Rebecca Aechtner, The Revd Dr Anderson Jeremiah, and all the Lancaster people. Thank you for the friendship and support for me and my family, I am blessed to be part of the Lancaster Priory.

Last but not least, I would like to dedicate this acknowledgement to my family. All the hard work, love and understanding that you gave was the best support for me, to enable me to finish this thesis. Thank you for the prayers that shade and guard me during my stay in Lancaster, UK. Ken Nararya Amurwabhumi and Kaia Amaris Swarnabhumi, the precious gifts from Jesus Lord in my life, I love you. The Lord gave me more than I asked for. I dedicate this thesis to you.

"He has made everything beautiful in its time."
Ecclesiastes 3: 11

Contents

List of Abbreviations

ACAS – Advisory, Conciliation & Arbitrase Service
AGS – Anuual Growth Survey
ALMPs – Active Labour Market Policies
CaaS – Communiaction as a Service
CMA – Computer Misuse Act
CSS – Corporate Strategic Scenario
DPA – Data Protection Act
DPO – Data Protection Officer
DRC – Disaster Recovery Center
ECI – European Cloud Initiative
ECP – European Cloud Partnership
EDPB – European Data Protection Board
EEA – European Economic Area
EIBN – EU-Indonesia Business Network
ENISA – European Network and Information Security Agency
ESO – Electronic System Operator
ETS – European Treaty Series
ETSI – European Telecommunications Standards Institute
EU – European Union
GCG – Good Corporate Governance
GDPR – General Data Protection Regulation
GTP – Global Talent Program
HR – Human Resource
IaaS – Infrastructure as a Service
ICO – Information Commissioner's Office
ICT – Information Communication and Technology
IDC – International Data Corporation
Id-SIRTII/CC – Indonesia's Security Incident Response Team on Internet and Infrastructure/ Coordinator Center
ISMS – Information Security Management System
ISO/ IEC – International Standards Organisation/ International Electrotechnical Commission
ITU – International Telecommunication Union
NaaS – Network as a Service
NITS – National Institute of Standard & Technology
PaaS – Paltform as a Service
PDR – Personal Development Review
Saas – Software as a Service
SLA – Service Level Agreement
SNI – Standard Nasional Indonesia
SOEs – State Owned Enterprises
UK – United Kingdom
WP – Working Party

Table of Figures

Chapter 1. Introduction, Aims and Objectives

1.1 Introduction

Technological advances and related shifts in required workforce skills have had a fundamental effect on the nature of economic development.[1] Investment in technology such as cloud computing is expected to bring a widerange of benefits to companies by improving productivity, innovation, speed and efficiency of processes.[2] Indonesia, with high expectations of the Information and Communications Technology (ICT) industry in South East Asia, is facing a range of ICT regulatory issues.[3] The Indonesian government regarding Guidelines and A Five-Year Action Plan for the Development and Implementation of ICT in Indonesia[4] has forced all sectors in Indonesia to use updated ICT as a support to business and infrastructure.[5] It further stated that the Indonesian government should use ICT to support good governance and to facilitate society to participate in the implementation and development of technology. Later it will be discussed how the ICT companies in Indonesia support the Indonesian government's vision of education and of supporting the development and empowerment of ICT in Indonesia. The implementation of technology has given rise to a number of legal issues related to the technology itself and the readiness of human resources to implement it.[6]

In 1990, the United Kingdom faced the reality that employees should be ready to overcome the challenges presented by the implementation of technology.[7] However, the European Union (EU), as a binding source of United Kingdom (UK) law, has

---

[1]Jaewon Jung, 'Technology, Skill, And Growth in A Global Economy' (*Econpapers.repec.org*, 2015) <http://EconPapers.repec.org/RePEc:ema:worpap:2015-08> accessed 5 October 2015.
[2] Joe Weinman, 'The Strategic Value of The Cloud' (2015) 2 IEEE Cloud Computing.
[3]Ali Rokhman, 'E-Government Adoption in Developing Countries; The Case of Indonesia' (2011) 2 Journal of Emerging Trends in Computing and Information Sciences <http://www.cisjournal.org/archive/vol2no5/vol2no5_4.pdf> accessed 5 October 2015.
[4] Indonesian Presidential Instruction 6/2001 regarding Guidelines and A Five-Year Action Plan for the Development and Implementation of ICT in Indonesia.
[5]Budi Hermana and Widya Silfianti, 'Evaluating E-Government Implementation by Local Government: Digital Divide in Internet Based Public Services in Indonesia' (2011) 2 International Journal of Business and Social Science <http://www.ijbssnet.com/journals/Vol._2_No._3_[Special_Issue_-_January_2011]/18.pdf>accessed 5 October 2015.
[6]Ibid. (n 1).
[7]Peter Cressey and Peter Scott, 'Employment, Technology and Industrial Relations in The UK Clearing Banks: Is the Honeymoon Over?' (1992) 7 New Technology, Work and Employment.

recommended in Active Labour Market Policies (ALMPs)[8] that there should be a policy related to the capability of the employee by the development of technology in the workplace. They emphasised some programmes including re-skilling and up-skilling to overcome the skill shortages. This is to encourage young people with a lack of experience, older workers and low-skilled people to improve themselves to achieve such skill in the workplace. The European Union Com (2014) 130[9] also recommended a strategy relating to smart, sustainable and inclusive growth. It stressed the importance of the readiness of employees, including training to improve their skills in the development of technology to support the sustainability of the industry.

This thesis has two overarching aims:

1. To analyse the extent to which the Indonesian cloud computing industry would be affected by wide-ranging data protection and data security law reforms.
2. To evaluate the potential impact that data protection and data security law reform could have on the position of employees in the Indonesian cloud computing industry.

The objective of this thesis is to evaluate the data security and data protection frameworks in the light of the implementation of cloud computing in the workplace. This objective will be achieved through an in-depth analysis of relevant EU and Indonesian law. This objective is also complemented by interviews with eleven relevant policy makers in Indonesia ICT companies.

The thesis will examine the Indonesian ICT companies by looking through their policies and the contribution of the policy makers in making policy in the companies. It will concentrate on aspects of technological regulations that support the development of cloud computing in the workplace, such as data security and data protection. By examining those regulations, it will reveal to what extent Indonesian regulation has supported employees on data security and data protection. The study is original as the researcher is researching the phenomena that occur in a workplace

---

[8] 'European Semester Thematic Factsheet - Active Labour Market Policies' (*Ec.europa.eu*, 2018) <https://ec.europa.eu/info/sites/info/files/file_import/european-semester_thematic-factsheet_active-labour-market-policies_en.pdf> accessed 20 January 2018.

[9] ''Taking Stock of The Europe 2020 Strategy for Smart, Sustainable and Inclusive Growth, COM(2014) 130 Final/2'2' (Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, 2014) <http://ec.europa.eu/europe2020/pdf/europe2020stocktaking_en.pdf> accessed 11 October 2015.

within which the researcher is uniquely placed to gain novel insights.This thesis also examines the perceptions of policy makers on the need to address the gap in skills created by the growth of the cloud computing industry. It reveals how policy makers overcome the skills gap in the workplace and determines whether the regulationsare enough to support the development of the cloud computing industry, especially related to data security and data protection, and makes recommendations related to the law and regulation in Indonesia.

Since the Indonesian Ministry Regulation 4/2016 regarding Information Security Management System in data security[10] and Indonesian Ministry Regulation 20/2016 regarding Personal Data Protection in Electronic System[11] were only promulgated in 2016, this thesis will also reveal how policy makers address the implementation period of the new regulations in policy-making in the companies. The current regulations and the establishment of the Indonesian National Cyber Security Organisation[12] in Indonesian Presidential Decree 53/2017 regarding National Cyber And Crypto Agency in 2017 have made this thesis important, since no-one has studied this topic before and it is the right time to examine such regulations in Indonesia. With the new European Union General Data Protection Regulation (GDPR) that came into force on 25 May 2018, it makes this thesis germane to phenomena that arise in the ICT industries concerning data security and data protection.

Policy makers need to be aware of the aspects that related to the development of technology to support companies. Policy, according to Black's Law Dictionary[13] is a law, or rule of lawand a policymaker is the person in the organisation who responsible for formulating policy.[14] These policy makers are in a position to focus on improving the skills of a company's employees, enhancing their personal value or social contribution as part of the company strategy. Therefore, the perceptions of policymakers will be used to bring greater insight to analysing the legal phenomena that have risen during the development of cloud computing.

---

[10] Indonesian Ministry Regulation 4/2016 regarding Information Security Management System
[11] Indonesian Ministry Regulation 20/2016 regarding Personal Data Protection in Electronic System
[12] Indonesian Presidential Decree 53/2017 regarding National Cyber And Crypto Agency
[13]Henry Campbell Black, Joseph R Nolan and Jacqueline M Nolan-Haley, *Black's Law Dictionary* (West 1990).
[14]Colin Yallop, *Macquarie Dictionary* (Macquarie Library 2005).

This thesis uses semi-structured interviews to examine the conditions in the ICT companies through responses from policy makers in the technological and human resources areas. The ICT companies are related to technology as their core business and human resource or employees as person who work in the industry. The policy makers in this thesis were the senior management who have the expertise in their work field, and could approve the draft of a policy before it was approved by the directors of their company. This is unprecedented access to policymakers in a unique institution, because the researcher is an employee of the company, which has funded the researcher, and alsobecause policy makers are directly chosen by the related director; and the institutions are also unique because the research is conducted in the biggest state-owned company in Indonesia and its subsidiaries. However, since this thesis examined the policy that related to technology and human resources in the company, not all the policy makers in the department in the companies were interviewed. Therefore, the purpose of the selection of the relevant policy makers in the Indonesia ICT company is in line with the objective of the thesis. Those areas were chosen because, before 2016, Indonesia did not have regulations on data security and data protection. The regulations are important to support the development and implementation of cloud computing in the ICT companies, as stated in the companies' strategic plan, and this required greater employee readiness and knowledge in the field of data security and data protection.

It is important for companies to update and improve the skill of their employees to meet the changes in the workplace.[15] By improving employee competencies, they can lower cost and achieve better quality and flexibility.[16] The Global Competitiveness 2013 – 2014 Report[17] stated that there are three sub-indexes which reflect the global competitiveness of a nation. First, basic requirements (institutional, infrastructure, the environment, health). Secondly, efficiency enhancers (education/training, product, employee, financial, technological readiness, market) and finally innovation and

[15]Nader Barzegar and Shahroz Farjad, 'A Study on the Impact of On the Job Training Courses on the Staff Performance (A Case Study)' (2011) 29 Procedia - Social and Behavioural Sciences.
[16]W. Yu and R. Ramanathan, 'Business Environment, Employee Competencies and Operations Strategy: An Empirical Study of Retail Firms in China' (2012) 24 IMA Journal of Management Mathematics.
[17]Klaus Schwab, *the Global Competitiveness Report 2013-2014* (World Economic Forum 2013).

sophistication (business and innovation). Companies with established infrastructure, adequate employees, strong finances and business continuity and innovation are more likely to be a leader in the industry. Participating in building these three sub-indexes to global competitiveness can improve the quality of the company through the basic requirements, of the employee through efficiency enhancements and the environment through innovation and sophistication.

However, there should be a legal framework under pinning the strategy. A legal framework for global competitiveness is required so that the company has a reference. It is in the best interest of companies and the executive authority of government. The law plays a role in many functions in the development of a nation.[18] Regulations have become the guardiansof fair practices to support the economic growth of a nation.[19] Regulations have become the keepers for the business player to avoid them becoming too dominant in the market.It should set the regulation and legal certainty for the market player, it should ensure the market player meets the regulations related to the business,[20] employees[21] and the environment,[22] and it should provide legal counsel related to new technology[23] and innovation.[24]

This thesis examines Indonesian regulations using EU and UK regulation. The EU implemented data security and data protection prior to the Indonesian regulations in Directive 95/46/EC[25] ('The Protection of Individuals with Regard to The Personal Data and On the Free Movement of Such Data') on 24 October 1995, and it has been

---

[18]Samuel D. Brickley 2nd and Brian M. Gottesman, 'Business Law Basics' (*Businesslawbasics.com*, 2016) <http://www.businesslawbasics.com/business-law-basics> accessed 5 October 2015.
[19] Murali Krishna Medudula, Mahim Sagar and Ravi Parkash Gandhi, 'Telecom Players, Regulatory Bodies, International Organisations and Regional Telecom Statistics: Global Overview' [2016] Telecom Management in Emerging Economies.
[20] Derek Stimel and Leslie E. Sekerka, 'Play Fair! Innovating Internal Self-Regulation in The Market for Profit' (2018) 61 Business Horisons.
[21] Smaranda Pantea, Anna Sabadash and Federico Biagi, 'Are ICT Displacing Workers in The Short Run? Evidence from Seven European Countries' (2017) 39 Information Economics and Policy.
[22] Colin Pattinson, 'ICT And Green Sustainability Research and Teaching' (2017) 50 IFAC-PapersOnLine.
[23] Max Parasol, 'The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, And on China's Big Data and Smart City Dreams' (2018) 34 Computer Law & Security Review.
[24] Ingo Vogelsang, 'Regulatory Inertia Versus ICT Dynamics: The Case of Product Innovations' (2017) 41 Telecommunications Policy.
[25]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

updated in Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation),[26] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA,[27] and Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for A High Common Level of Security of Network and Information Systems Across the Union.[28] Those protections indicate that the EU has given a sufficient protection to its members. To have sufficient protection in companies, policy makers need to be aware of the obstacles that occur in companies. These could be from the outside or inside the companies. The obstacles outside the companies might arise when there is not enough protection through regulation related to the company's business, which is to make sure that companies have already provided the legal certainty related to the business, whilst the inside problem might relate to the knowledge and readiness of employees to implement the company's policy related to the adoption of new business strategy in the company. Therefore, the expertise and experiences of the policy makers is critical in adjusting the company objectives and the employees' requirements to comply with such regulations.The researcher also wanted to probe the reality of the actual experiences and insights gained in these companies to be able to evaluate the substance of the law more effectively.

Companies need to adjust their business strategy to ensure that they are able to

---

[26] EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).
[27] EU Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA.
[28] EU Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for A High Common Level of Security of Network and Information Systems Across the Union.

compete in the market.[29] For ICT companies, it is important for them to improve their services so they can be leaders in the constantly developing market. To be able to do that, sufficient knowledge is required by ICT employees.[30] These considerations have created more challenging conditions for companies and employees to survive in the industry.[31] The right people in the right places are needed to prepare the company for the changes that are caused by technology,[32] which involved innovations and skills in the ICT industry, especially related to the rapid development of technology. The development of technology in the workplace has made employees change their perspective on their work.[33] The new trend of using cloud computing as a business model has brought a new paradigm that requires employees to be more technologically literate.[34] However, the needs of technological literacyare not merely related to the technological aspect, but also to the impact of the implementation of the new technology. In this thesis, the focus is on the effect of the data security and personal data protection in the workplace, which has legal aspects. To support that, proper approaches by policy makers are needed, for example in highlighting the importance of data security and data protection in the workplace. Targeted training for employees will create a positive effect on the company.[35] Policy makers should consider to what extent the impact of training will enhance the capability of the employee, how effective is the training, and how companies will prepare the employees with different levels of capacity and knowledge to overcome the implementation of data security and data protection in cloud computing. Furthermore, the policy makers should consider the regulations provision related to the implementation of data security and data protection with the preparedness of the employees to encounter the development of technology in the workplace.

It is important for ICT employees to realise that they have a huge responsibility to

---

[29]Ibid. (n 2).
[30]Ibid. (n 15).
[31]Katarina Stanoevska-Slabeva, Thomas Wozniak and Santi Ristol, *Grid and Cloud Computing* (Springer 2010).
[32]Witold Abramowicz, *Business Information Systems Workshops* (Springer 2014).
[33]Michael D Coovert and Lori Foster Thompson, *the Psychology of Workplace Technology* (Routledge 2014).
[34]Zahir Tari et al., 'Security and Privacy in Cloud Computing: Vision, Trends, and Challenges' (2015) 2 IEEE Cloud Comput.
[35] Ravi Bapna et al., 'Human Capital Investments and Employee Performance: An Analysis of IT Services Industry' (2013) 59 Management Science.

maintain the data security and personal data protection in the workplace, not only for the interest of the company and customer, but also for the benefit of the employees themselves. ICT companies hold personal data that should be protected and the companies' systems must provide data security to protect that personal data.

A study[36] has shown that cybercrime in Indonesia has risen massively since 2003. Kizza[37]argues that employees might have great potential to become cyber criminals, as they have the authority to access the system in the workplace. ICT companies that keep personal or sensitive data of their customers and employees must be aware of the importance of securing the data. The aim of policy-making is to solve a need by outlining the problem and implementing the laws and policies to achieve the solution.[38] Policy makers could improve the ability of the employees through training. Moreover, it is mandated by Indonesian regulation[39] that:

> 'Job training shall be carried out by taking into account the need of the job market and the need of the business community, either within or outside the scope of employment relations. Job training shall be provided on the basis of training programs that refer to job competence standards'.

Therefore, policy makers should be able to provide for the need of the employees to be able to compete in the market. Further the regulation[40] stated that 'Manpower has the right to acquire and/or improve and/ or develop job competence that is suitable to their talents, interest and capability through job training'. The regulation has thus stated that it is the right of the employees to have training to support them in the workplace.

In relation to the implementation of data security, the International Standards Organisation and International Electrotechnical Commission (ISO/IEC) 27001 stated that:

> 'The organisation needs to ensure that staff are aware of information security

---

[36]'History of ID-SIRTII/CC' (*Idsirtii.or.id*) <http://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html> accessed 3 February 2017.
[37] Joseph Migga Kizza, *Guide to Computer Network Security* (Springer 2015).
[38]Marijn Janssen and Natalie Helbig, 'Innovating and Changing the Policy-Cycle: Policy makers Be Prepared!' [2016] Government Information Quarterly.
[39] Indonesian Act 13/2003 regarding Manpower, Article 10(1).
[40]Ibid, Article 11.

> risks and have sufficient understanding to support the organisation's information security policy to undertake their normal work functions and tasks. Staff should be trained in the use of information security policies and procedures, security controls applicable to their job function and the correct use of IT (e.g., log in procedures, keeping passwords safe, appropriate use of IT)'.[41]

The main service of the ICT business is related to how ICT companies make sure that by using the companies' equipment, the data kept by ICT companiesis securely saved. This covers not only the companies' data, but also customer data and employees' data. This means ICT companies have to make sure that they have a reliable data security and they have trusted employees to maintain the personal data in the companies' premises. Employees need to make sure that the data kept in their premises is save and confidential. This is the reason why employees in ICT companies need to be aware and updated with the policy and regulation related to data security and data protection.

As stated previously, the Indonesian regulations were published in 2016 but they did not stop companies to expand the business in cloud computing. Moreover, policy makers should be able to overcome the implementation period of the regulation. This thesis has also examined the policy makers' support to the implementation of cloud computing in Indonesia due to the implementation period of the new regulations. It became an important challenge for policy makers to support the companies' objective with the regulations, or in this thesis future regulations. Policy makers should communicate with the regulator intensively in the companies' interest or by giving input related to the implementation of technology.

Section 1.2 will discuss the extent to which cloud computing would be affected by wide-ranging data protection and data security law reforms, and then Section 1.3 will discuss the potential impact of data protection and data security on Indonesian ICT employees and the cloud computing industry. Section 1.4 will examine the extent of ICT companies' readiness for the implementation of data security and data protection in the Indonesia cloud computing industry.

---

[41] Edward Humphreys, Implementing The ISO/IEC 27001 ISMS Standard, Second Edition (Artech House 2016).

1.2 Data Security and Data Protection in Cloud Computing

The development of technology in telecommunication has brought numerous benefits.[42] Technology has shortened distances, speeded up communication, and simplified connections. People are now using sophisticated communications technology in all aspects of life. Technology has caused a significant shift in the ICT industry.[43] The ICT industry should be able to meet market needs. For example, in the health system, they have built up cooperation with hospitals to deliver e-health,[44] which includes health insurance, medicine and doctors' services. The ICT industry's business strategy should be ahead of the market requirement. ICT companies need to offer a diverse service product in addition to their main core business.

One recent development in the ICT industry is cloud computing. Definition from the National Institute of Standard and Technology (NIST), which has been referenced by industry-wide,[45] stated that cloud computing:

> '[i]s a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'.[46]

Using cloud computing, they have outsourced the function of capacity, security, and maintenance into a company database.[47] All in one system, so that companies with extensive data can divert their budget elsewhere. Cloud computing is frequently used in banking,[48] airlines,[49] and many other companies that require an enormous database

---

[42]M. Cardona, T. Kretschmer and T. Strobel, 'ICT and Productivity: Conclusions from the Empirical Literature' (2013) 25 Information Economics and Policy.
[43]Rosalind Williams, 'The Lantern-Bearers of The History of Technology' (2013) 29 History and Technology.
[44]Paul Wicks et al., 'Innovations in E-Health' (2013) 23 Quality of Life Research.
[45]Lizhe Wang, *Cloud computing* (1st edn, CRC Press 2012).
[46]National Institute of Standards and Technology, 'The NIST Definition of Cloud Computing' (Computer Security Division, National Institute of Standards and Technology 2011).
[47]Divya Bhatt, 'A Revolution in Information Technology - Cloud Computing' (2011) 9 Walailak Journal of Science and Technology (WJST) <http://wjst.wu.ac.th/index.php/wjst/article/view/25/203> accessed 10 May 2015.
[48] W. Kuan Hon and Christopher Millard, 'Banking in The Cloud: Part 2 – Regulation of Cloud As 'Outsourcing' (2018) 34 Computer Law & Security Review.
[49] Vagdevi P and H S Guruprasad, 'A Study on Cloud Computing in Aviation and Aerospace' (2015) 6 International Journal of Computer Science & Engineering Technology (IJCSET).

for their activity.[50]

Cloud computing as a technology has been responded to immediately by the public for its simple connectivity and procedure.[51] It is a new service business model that has been created to assist people to do their business. It makes them work faster (because it is limitless), more easily (because it is standardised) without necessarily spending a lot of money on the system. The term 'cloud computing' was introduced by telecommunication operators in the early 1990s to determine the responsibilities between users and providers. However, it was Amazon Web Services that promoted the term, so that became widely used as it is today.[52]

Stitilis and Malinauskaite[53] stated that cloud computing is a system in which the provider kept the end user's data in their hardware which is maintained by the provider. Whenever the user wants to access the data, they can easily connect and access the server and adjust the amount of the hardware as required. The provider will secure and maintain the data which is kept on their system. The data saving system is outsourced to the provider so that the user can pass on the obligation of maintaining and securing their data. It is easier and more convenient to the user since the cloud computing system enables them to access their data whenever they choose, and it does not incur a high maintenance cost. Users choose cloud computing for its benefits; they can easily access their data through the internet as they need it, and only pay for what they use.[54] Soon cloud computing became known as the simplest way to reduce activity and expenditure, and companies began to introduce cloud computing as their

---

[50] Keng-Boon Ooi et al., 'Cloud Computing in Manufacturing: The Next Industrial Revolution in Malaysia?' (2018) 93 Expert Systems with Applications; S.K. Chaulya and G.M. Prasad, 'Application of Cloud Computing Technology in Mining Industry' [2016] Sensing and Monitoring Technologies for Mines and Hazardous Areas; Robert K. Perrons and Adam Hems, 'Cloud Computing in The Upstream Oil & Gas Industry: A Proposed Way Forward' (2013) 56 Energy Policy.

[51] Eric Bauer and Randee Adams, *Reliability and Availability of Cloud Computing* (Wiley-IEEE Press 2012).

[52] Primavera Filippi and Smari McCarthy, 'Cloud Computing: Centralisation and Data Sovereignty' (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/101/245> accessed 5 October 2015.

[53] Darius Stitilis and Inga Malinauskaite, 'Compliance with Basic Principles of Data Protection in Cloud Computing: The Aspect of Contractual Relations with End-Users' (2014) 5 European Journal of Law and Technology <http://ejlt.org/article/view/231/422> accessed 5 August 2016.

[54] George Reese, *Cloud Application Architectures* (O'Reilly 2009).

new business model.[55]

Any level of user can use cloud computing, from individual to corporate, depending on their purposes. The use of cloud computing depends on the capacity required by the user. There are three service layers in cloud computing that are being offered.[56] Each service delivers different capacity and usability.

The first is Infrastructure as a Service (IaaS).[57] When the user uses this service, they are allowed toaccess the storage, hardware, servers, and network components. The infrastructure can be upgraded or downgraded as required. The second service is Platform as a Service (PaaS). This service is often used by customers who are already aware of the system technology and large companies will use this service. It allows the customer to build, assess and organise their applications. The third service is Software as a Service (SaaS). This supports bespoke software. The user might be able to access this application remotely and to share files with several devices at the same time.[58]

Besides the grouping of service delivery, in cloud computing there are also groupings based on deployment of the service:[59] public clouds, in which all the operational system is completed and checked daily by the vendor;private clouds, in which all functions completed by the user; and hybrid clouds, in which only vital data is held by the user; and lastly, community clouds; which are based on a community or organisation that has a specific mutual concern.[60]

Uses need to understand some aspects before choosing cloud computing as their

---

[55]Adel Nadjaran Toosi et al., 'Revenue Maximisation with Optimal Capacity Control in Infrastructure as a Service Cloud Markets' (2015) 3 IEEE Transactions on Cloud Computing.
[56]Hoang T. Dinh et al., 'A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches' (2011) 13 Wireless Communications and Mobile Computing.
[57]Sushil Bhardwaj, Leena Jain and Sandeep Jain, 'Cloud Computing: A Study of Infrastructure as A Service (Iaas)' (2010) 2 International Journal of Engineering and Information Technology.
[58]Christof Weinhardt et al., 'Cloud Computing – A Classification, Business Models, And Research Directions' (2009) 1 Business & Information Systems Engineering.
[59] Bhavani Thuraisingham, A Comprehensive Overview of Secure Cloud Computing (2012).
[60]Timo Leimbach et al., 'Potential and Impacts of Cloud Computing Services and Social Network Websites' (*European Parliamentary Research Service*, 2016).<http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf> accessed 9 July 2016.

business model. Teneyuca[61] explained that there were a number of concerns on cloud computing before parties are ready to sign the contract. These are often associated with the rights of user access, regulatory compliance, data location, data splitting and separation, data recovery, investigative maintenance and long-term sustainability. Stitilis and Malinauskaite[62] pointed out that the principles of data removal, privacy, access availability, integrity, and indemnification are the significant issues that the user must be aware of. Bodei[63] emphasised the two central issues in a cloud computing contract as integrating process and security issues relating to the applications and systems. Monteleone[64] highlighted that personal information, privacy, and identity were the principal subjects to be raised whenever parties agree a contract for cloud computing. Reese[65] thought that users are should be aware of data security, including the data maintenance by the provider, data recovery related to error or hackers, data encryption, regulatory compliance, and network security (firewall and network traffic, antivirus, data management). Most of these thoughts above are concerning two significant issues related to the clause in the contract of cloud computing. First is the data integration process from provider to user and the second is data security.

Recently, other issues have arisen. One is about the jurisdiction and legal system of cloud computing and the other is about the accessibility of data and the standard contract on cloud computing.[66] The jurisdiction issues appear when the providers are not in the same country as the user, or the user might not even know where the provider is. This is important for the cloud business, since the customer needs to be sure that their data has been protected securely and not transferred to another party without consent. Using standard contracts means that provider and user are forced to agree on the content of the contract. This circumstance does not benefit the user

---

[61]David Teneyuca, 'Internet Cloud Security: The Illusion of Inclusion' (2011) 16 Information Security Technical Report.
[62]Ibid. (n 53).
[63]Chiara Bodei et al., 'Security in Pervasive Applications: A Survey' (2013) 4 European Journal of Law and Technology <http://ejlt.org/article/view/276> accessed 10 October 2015.
[64] Shara Monteleone, 'Privacy and Data Protection at the Time of Facial Recognition: Towards a New Right to Digital Identity?' (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/168/257> accessed 5 May 2016.
[65]Ibid. (n 54).
[66] Karen McCullagh, 'Response to EU Commission Public Consultation on Cloud Computing' (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/137/228> accessed 22 July 2016.

because they have no bargaining position in this situation. The terms of the contract are already settled. The user has to accept the conditions established by the provider. However, many terms related to the cloud computing service need to be clarified by both parties. In a contract for cloud computing, there should be an explicit condition related to the rights and obligations of parties since the essence of the cloud computing agreement is being transferred on those terms.

Nowadays, cloud computing has become one of the promising businesses in the world.[67] Google, Parallels and Virtustream have become the three top companies to work for in the world.[68] In Indonesia, Telkomsel, the largest cellular operator and the sixth largest in the world, has used the cloud as their part of the business.[69] It has been shown in Indonesia that the use of cloud computing has influenced telecommunications and especially the ICT business. Telkomsel, Telkomsigma and PT Telkom are the companies that were the source of the data resources in this thesis. Telkomsigma, one of the biggest cloud computing companies in Indonesia, has recently signed a contract with PT IBM Indonesia as part of expanding their service to customers, which is aligned with their business strategy. Telkomsigma was acquired by a subsidiary of PT Telkom Indonesia, Tbk (Telkom). The cooperation is intended to provide the central capacity in the industrial sector in Indonesia. The collaboration between Telkomsigma and IBM was made to support the desire of Telkom to be the leading telecommunication provider.[70] Telkomsigma plans to build the largest Disaster Recovery Centre (DRC) Park to protect the customer data centre in the event of an earthquake. They realised that the company needed to increase its capability in order not to struggle in the market. The development of technology has to lead the business strategy of the company so that the company might have survived in the competition. Companies need to change radically, especially on the performance of their services to give the best for their customer.

---

[67]Louis Columbus, 'The Best Cloud Computing Companies and Ceos to Work for in 2015' (*Forbes.com*) <http://www.forbes.com/sites/louiscolumbus/2015/01/29/the-best-cloud-computing-companies-and-ceos-to-work-for-in-2015/> accessed 10 October 2016.
[68]Ibid.
[69]Faisal Gandi, 'Cloud Computing Set to Dominate Corporate Internet Services' (*The Jakarta Post*, 2014) <http://www.thejakartapost.com/news/2014/04/29/cloud-computing-set-dominate-corporate-internet-services.html> accessed 28 October 2015.
[70]'IT Consulting Services & System Integration - Telkomsigma' (*Telkomsigma*) <http://www.telkomsigma.co.id/it-consulting-services-system-integration/> accessed 10 October 2016.

To implement cloud computing in the workplace, companies should consider the flexibility, scalability and the potential for innovation and mobility from cloud computing as it can reduce their expenditure. Cloud computing has brought a new style of life with its mobility and accessibility.

Cloud computing has contributed to a positive environment because it can reduce pollution and help with energy saving. For example, in a meeting, people might use data that is being kept and shared in the cloud database to reduce the use of paper in the office. The provider can also provide the user with many benefits from its data securing and business sustainability, in particular for a company that is not familiar with cloud computing.[71] However, there is still debate as to what extent the provider will provide for the safety of the user's data.[72] Another consideration is related to the transfer of knowledge to maintain the sustainability of the user's employee and training on the latest technology. All of these concerns are related to the implications of cloud computing for a company's business model since particular skills in IT are essential to the company to sustain the business.

Even though the implementation of cloud computing still has debate on several factors, its use is becoming more popular.[73] The development of cloud computing itself has driven people to improveits performance and at the same time to regulate terms related to it.

The European Telecommunications Standards Institute (ETSI), the European Union Network and Information Security Agency (ENISA), and the working groups of the European Commission[74] have carried out research relating to the standard terms and the development of cloud computing. The International Telecommunication Union (ITU)[75] released a report in March 2012 relating to privacy in cloud computing.

---

[71]Ibid. (n 54).
[72]Ibid. (n 56).
[73]Ivonne Sartika Mangula, Inge van de Weerd and Sjaak Brinkkemper, 'Adoption of The Cloud Business Model in Indonesia' [2012] Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services - IIWAS '12.
[74]Niamh Gleeson and Ian Walden, 'It's A Jungle Out There'? Cloud Computing, Standards and the Law' (2014) 5 European Journal of Law and Technology <http://ejlt.org/article/view/363/461> accessed 5 October 2015.
[75]Stéphane Guilloteau and Venkatesen Mauree, 'Privacy in Cloud Computing' (*ITU-T Technology Watch Report*, 2012) <https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf>

Efforts have been made to form legal terms in cloud computing, especially related to the technological issues such as data protection, data security, interoperability, data portability, reversibility and Service Level Agreements (SLA).

Issues in using cloud computing are divided into technical (application including transmission and entities) and territorial (related to the multi jurisdictional aspects of the user and provider).[76] This thesis will discuss issues related to the technical, which is data security, and the territorial, which data protection. It also examines the implementation of cloud computing in ICT companies. ICT companies play a big role in cloud computing in Indonesia. The ICT companies in this thesis provide and use cloud computing. It is important for such companies to make sure that they have complied with the regulations before marketing their product, and that their employees are aware of the aspects of the implementation of cloud computing in their companies.

It is important for the policy makers to make sure that the ICT employees has aware of and comply with the regulation in data security and data protection, since they will be dealing with the data of the employees themselves and the data of the customers. The regulations and policies compliances are to prevent errors in the companies made by its employees. Policy makers should make sure that their policy will protect the employees, customers and the companies themselves. They need to be assured that the ICT employees will comply with the regulation and policy.

1.3 The Potential Impact in the Workplace from the Implementation of Legal Aspects of Cloud Computing

To be able to support the development of technology, ICT employees should be prepared with adequate skills and knowledge to overcome the gap caused by technology. They must understand that they carried a huge responsibility in keeping the data safe, not only the company's data, but the customers' data as well. Therefore, policy makers should realise that it is important for ICT companies to provide employees with adequate skills and competence to cope with the development of technology in the workplace.

---

accessed 10 October 2015.

[76]Christopher J Millard, *Cloud Computing Law* (Oxford University Press 2013).

Annually the EU collects data on general economic priorities through the Annual Growth Survey (AGS),[77] which offers some policy guidance for the following year. The AGS is important as it captures three important aspects in economic development; investment, structural reforms and fiscal consolidation.[78] EU members, stakeholders and social partners should build the same perspective to succeed the implementation of the policy. However, it is important that not only the EU members, but also EU partners have an understanding of the importance of the priorities and the guidelines in the AGS.[79] Therefore, Indonesia, as an EU partner in commerce,[80] should be aware to the EU's long-term growth strategy Europe 2020.[81]

In the 2013 EU AGS,[82] it was explained that it is important to match the job with the proper skills and competencies, especially in supporting the 'future job'. The future job, according to the AGS, is one related to environment, health and ICT. A mismatch between the employees' skill and knowledge with the job may affect the company's strategy in the market. The AGS explained that there are two types of skills mismatch. One is the skill deficit or skill gap, when an employee does not match the job requirements. The other is skill under-use, when the employee is skilled beyond the requirements of the job. In the recruitment process, the perspective employees are placed in accordance with the job applications. However, occasionally employees should be able to work outside their skill.

Employees should be ready and prepare themselves with sufficient skill and companies play a big role in improving the skill of their employees through the

---

[77]'Annual Growth Survey 2018' (*European Commission*, 2018) <https://ec.europa.eu/info/sites/info/files/2017-comm-690_en_0.pdf> accessed 28 June 2018.
[78]'Setting the Priorities' (*European Commission*, 2018) <https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/european-semester-timeline/setting-priorities_en> accessed 28 June 2018.
[79]'The Autumn Package Explained' (*European Commission*, 2018) <https://ec.europa.eu/info/sites/info/files/the-autumn-package-explained_en.pdf> accessed 28 June 2018.
[80]'Indonesia Growth Opportunity and Market Expansion' (*Eibn.org*) <http://eibn.org/> accessed 21 March 2018.
[81]Ibid. (n 79).
[82]'Skills Mismatches and Labour Mobility' (*European Union*) <http://ec.europa.eu/europe2020/pdf/themes/27_skills_gaps_and_labour_mobility.pdf> accessed 10 October 2016.

facilitation of training.[83] Nowadays, ICT companies tend to hire people with more education and skill.[84] As the consequence of improving skill qualification, the employees' turnover is relatively high. SamGnanakkan[85]stated that turnover is caused by the shortage of experience and the high cost of training in companies. If we look at those statements, the turnover of the ICT employees is relatively high along with the rapid development of technology. It is the policy of the companies to have the employees' turnover, however, companies should provide those employees with an adequate skill so that they can have a maximal productivity in the new workplace. ICT employees themselves should improve and provide themselves with adequate knowledge and experience so they can survive in the workplace.

If we look at the AGS policy in the proposal on the guidelines for the employment policies,[86] it is stated that EU members should promote the employment strategy on supporting a skilled, trained and adaptable workforce to promote economic change. The employment strategies are to support the improvement of the workforce to have more skill and function, and to promote equal opportunity in the workplace.[87] One of the purposesof the AGS policy is to support potential job creation in ICT.[88] Therefore, ICT companies play a big role in the Europe 2020 Strategy for smart, sustainable and inclusive growth.[89] To have adequate knowledge, training is the best way for employees to improve their skills. This training is not only valuable for the company to upgrade the ability of employees, but also to identify and place the right employee in the right position, and to help deal with the skills mismatch that is concerning the

---

[83]Ibid. (n 15).
[84] Hugo Castro Silva and Francisco Lima, 'Technology, Employment and Skills: A Look into Job Duration' (2017) 46 Research Policy.
[85]Samson SamGnanakkan, 'Mediating Role of Organisational Commitment on HR Practices and Turnover Intention Among ICT Professionals' (2010) 10 Journal of Management Research.
[86]'Proposal for A Council Decision on Guidelines for The Employment Policies of The Member States' (*European Commission*, 2018) <https://ec.europa.eu/info/sites/info/files/2017-comm-677_en.pdf> accessed 28 June 2018.
[87]'European Employment Strategy - Employment, Social Affairs & Inclusion - European Commission' (*European Commission*, 2018) <http://ec.europa.eu/social/main.jsp?catId=101&intPageId=3427> accessed 28 June 2018.
[88]'Employment Package - Employment, Social Affairs & Inclusion - European Commission' (*European Commission*, 2018) <http://ec.europa.eu/social/main.jsp?catId=1039&langId=en> accessed 28 June 2018.
[89]'Europe 2020 Strategy' (*European Commission*, 2018) <https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_en> accessed 28 June 2018.

EU.[90]

SamGnanakkan[91] stated that training in ICT companies should be able to manage the needs of the training with organisational effectiveness, since the result of the training only affects ten percent of behavioural change in the workplace. Therefore, in policy-making related to employees benefits from training, policy makers should be able to determine the training priority according to the companies' strategy. If we compare this to the Indonesian Act Number 13 of 2003, it stated that:

> 'Job training is the whole activities of providing workers or potential workers with, and paving the way for them to acquire, enhance and develop job competence, productivity, discipline, work attitude and ethics until a desired level of skills and expertise that match the grade and qualifications required for a position or a job is reached'.[92]

The consequence of the provision is that companies should be able to provide their employees with sufficient skill and knowledge to reach the qualification in their workplace. In ICT companies, it could be interpreted that whenever there is a development in technology that influences the assignment of employees, companies should provide them with sufficient skills and knowledge. This interpretation is in line with the AGS policy stating that ICT companies should position themselves to avoid the problems associated with skills mismatch and prepare the workforce for the future.

In ICT companies, employees should be aware to the changes of recent technology before it is marketed to customers. A new technology in the workplace will bring a new environment to the employees. Townsend and Bennett[93] stated that technology has changed the behaviour of the company, as it has to adjust the work atmosphere, individual performance, organisation of the company, business strategy and employee interaction. Chesley[94] stated that technology in the company has affected the way employees do their jobs andhas increased workload and productivity. To be able to

---

[90]Kenneth A. Marentette, Alan W. Johnson and Lisa Mills, 'A Measure of Cross-Training Benefit Versus Job Skill Specialisation' (2009) 57 Computers & Industrial Engineering.
[91]Ibid. (n 85).
[92]Ibid. (n 39), Article 150-172, Article 1(9).
[93]Anthony M. Townsend and James T. Bennett, 'Information Technology and Employment Law: Challenges in an Evolving Workplace' (2003) 24 Journal of Labor Research.
[94]Noelle Chesley, 'Technology Use and Employee Assessments of Work Effectiveness, Workload, and Pace of Life' (2010) 13 Information, Communication & Society.

cope with the effect of the development of technology in the workplace, employees should adjust themselves to the new environment and companies should prepare them with sufficient and skills and knowledge so that the technology can be applied properly. This includes the implementation of legal aspects such as data security and data protection.

However, the ICT employees' preparation is not merely related to the technological aspects, but also to the legal aspects. The implementation of cloud computing is not merely related to the technological infrastructure issues such as the platform, software and hardware. ICT companies must update themselves with the newest developments in technology, since the service that they market is influenced by it. Therefore, ICT employees are being forced to improve themselves with the newest technology, but not all are willing and some are unenthusiastic. This could be caused by the age gap,[95] education gap[96] or lack of knowledge.[97] Even though those problems appear in the implementation of new technology, it does not mean that employees might reject the companies' strategy and policy which involves a new technology.

It is important for the ICT employees to support the companies' strategy and policy so that they can support the companies' business, and improve their knowledge of the latest technology. If we look at the Blue Book 2016 of EU-Indonesia Development Cooperation in 2015 (the Blue Book),[98] it stated that the EU and Indonesia will cooperate to build science and technology to meet today's global challenges, including data security and data protection regulations brought on by the implementation of cloud computing. This is a key legal issue that needs to be addressed.

ICT companies, through policy makers, should be able to classify the potential impact

---

[95]Sutrisno Hadi Purnomo and Yi-Hsuan Lee, 'An Assessment of Readiness and Barriers towards ICT Programme Implementation: Perceptions of Agricultural Extension Officers in Indonesia' (2010) 6 International Journal of Education and Development using Information and Communication Technology <http://files.eric.ed.gov/fulltext/EJ1085021.pdf> accessed 17 November 2017.
[96]Lukasz Arendt, 'Barriers to ICT Adoption in SMEs: How to Bridge the Digital Divide?' (2008) 10 Journal of Systems and Information Technology.
[97]Mahesha Kapurubandara and Robyn Lawson, 'Barriers to Adopting ICT And E-Commerce with SMEs In Developing Countries: An Exploratory Study in Sri Lanka', *Collaborative Electronic Commerce Technology and Research* (Collector Group 2006).
[98]'Blue Book 2016: EU-Indonesia Development Cooperation In 2015 - International Cooperation And Development - European Commission' (International Cooperation and Development, 2017) <http://ec.europa.eu/europeaid/blue-book-2016-eu-indonesia-development-cooperation-2015_en> accessed 16 February 2017.

of the implementation of cloud computing in the workplace by emphasising the importance ofunderstanding the implications for data security and data protection. There are some potential impacts that might be occur in ICT companies, especially related to the data security and data protection that might be done by the ICT employees, such as the cybercrime that involving customer's personal data and password breaching by employees. Policy makers should be able to make sure that their employees have the knowledge and responsibility in the workplace related to the implementation of cloud computing, especially related to the legal aspects of data security and data protection. However, some employees might not feel comfortable with such changes by the new policy, especially related to the implementation of new technology.

To overcome employee reluctance or if some employees do not feel they fit the position and the new environment in the workplace, beside training, companies might offer a retirement programme. This will be a win-win solution for both employees and companies. For employees, they can voluntarily take the programme without feeling they are disliked by the companies because of their incapacity, and the companies can hire some professionals to fill in.

As a comparator, the UK is a developed country with strong dismissal laws and robust protections. However, this allows for dismissal on competency grounds, which covers situations where there is a skills mismatch. If we refer to the UK Court of Appeal, it held in *Taylor v Alidair Limited*[99] that the employer was allowed to dismiss an employee for incapacity or incompetence. However, it will require reasonable grounds and good reasons. In *E C Cook v Thomas Linnell & Sons Limited*,[100] the Employment Appeals Tribunal stated that the incompetence of an employee can be a reason to dismiss them, if the dismissal follows adequate evidence and time.[101] Section 98 of the Employment Rights Act 1996 allows an employer to dismiss the employee based on their capacity as long as it is reasonable. Reasonable means that before the decision is made, there is fair assessment of the employee which can be done through competence

[99][1978] IRLR 82.
[100] [1977] IRLR 132.
[101]Peter Chandler, *An A-Z of Employment Law: A Complete Reference Source for Managers* (4th edn, Kogan Page Ltd 2003).

and skill or through leadership. Employee with a lack of skill or poor leadership can be considered not to fit with the companies' strategy.

Although it is legal to dismiss an employee for incompetence,[102] there are procedures that should be followed. According to the UK Advisory, Conciliation and Arbitration Service (ACAS) Code of Practice 1 – Disciplinary and Grievance Procedures,[103] the employer should notify the employee of the reason for the dismissal and should take the necessary steps to mitigate the reason. ACAS is the UK organisation that deals with the relationships between employers and employees and conciliates workplace problems. It is the company's obligation to obey the regulations that deal with employment issues to avoid unfair dismissal.

Even though under performing employees can be dismissed, there are several things that should be considered before the dismissal takes place. One of the considerations is related to the working period of the employee. The longer the period of employment, the more opportunity the employer should give him. This is because they have served the company and have invested more for the company through their work, especially if the reason of dismissal is because they cannot adapt to the new technology. The employer should look for a way to enhance the existing employee's capability. In *Tiptools Limited v T W Curtis*,[104] it was held that the employer is under an obligation to find an existing employee more suitable work or to look for necessary training to improve their ability.

However, not every country allows employers to dismiss their employees for lacking capability. In the Indonesian Act of Manpower, which is enacted in 2003, there is no clause which explicitly states that employees might be dismissed due to incapability or lack of skill. The clause in the Act of Manpower might be written as a letter of law, which as the consequence that incapability or lack of the skill cannot be the reason of sacking employee in the company. However, the clause of the Act of Manpower should also be written as the application of the law that due to the lack of

---

[102]Ibid.
[103]Advisory, Conciliation and Arbitration Service (ACAS), 'Code of Practice on Disciplinary and Grievance Procedures' (*Advisory, Conciliation and Arbitration Service*, 2015) <http://www.acas.org.uk/media/pdf/f/m/Acas-Code-of-Practice-1-on-disciplinary-and-grievance-procedures.pdf> accessed 11 March 2016.
[104][1973] IRLR 276.

incompetence in the company, ICT companies should support the employees in uplifting their skill and knowledge through training. Further, it is mandates[105] that companies should make a maximal effort to keep the employees in the company: 'The entrepreneur, the worker/labourer and or the trade/labour union, and the government must make all efforts to prevent termination of employment'. Companies should comply with the provisions of the Act, therefore, to avoid the termination, certain efforts should be made, such as by delivering training and qualifications to improve the skill of employees. Companies should not dismiss their employee except for the reasons stated in the Act of Manpower[106]and if the employee's termination happens for the reasons stated in the Act, they are entitled to compensation or benefits.[107]

For an ICT company, the need to improve skills related to new technology is inline with the company strategy. However, there are several requirements for the company before they approve training. The UK's Employee Study and Training (Procedural Requirements) Regulation 2010: 155, under section 63D of the Employment Rights Act 1996[108] states that to have approval for training, the employee should explain how the training will improve their skill, how it is related to the performance of the company, and to what extent the training is in line with the company strategy. However, there are several reasons that training application might be refused, which are:

a) 'That the proposed study or training to which the application, or the part in question, relates would not improve:
(i) the employee's effectiveness in the employer's business, or
(ii) the performance of the employer's business;
b) the burden of additional costs;
c) detrimental effect on ability to meet customer demand;
d) inability to re-organise work among existing staff;
e) inability to recruit additional staff;
f) detrimental impact on quality;
g) detrimental impact on performance;
h) insufficiency of work during the periods the employee proposes to work;
i) planned structural changes;

[105]Ibid. (n 39), Article 151(1).
[106]Ibid. (n 39), Article 150-172.
[107]Ibid. (n 39), Articles 153, 160(7), 161(3), 162(1), 164 (1-3), 165 – 168(1), 169 (1), 172.
[108] UK Employment Rights Act 1996, Part 6A, section 63D.

j) any other grounds specified by the Secretary of State in regulations'.[109]

This clause above states that, it is important for employee to always find out the suitable training and whether the employees' necessity and company Corporate Strategic Scenario (CSS) is fitted. In CSS, it is require that corporate planning is in line with the necessity of the company and the strategic plan for the development of the business, therefore, policy makers not only should formulate the business plan, but also should consider the readiness of the employee to support the company's strategic plan. In CSS, policy makers are formulated short- and long-term plan that are in corporate level, business level and functional level. It consists of strategic situation analysis, strategy formulation, strategy implementation, strategy evaluation and control, and risk profile analysis. It highlighted the external and internal analysis, vision, mission and strategic objective, the corporate strategy, financial and business projection and direction, management review, human resource policy, and potential risk and mitigation.

Telkom, in its CSS has affirmed that the policy makers are supporting the vision and mission of the corporate strategy by aligning its employees to be the best employees in the workplace through accelerating the capability of the employees with the development of digital. This could be achieved by mapping the competency development. Later, the policy makers should align the CSS with the human resource road map to formulate and detail some policies in human resource area. This could in the relation of developing a flexible organisation, building digital capability, or doing a professional hire. However, for budget saving, it is most likely that building digital capability is the best solution for the company.

This solution is also in line with the provision in Indonesian Act 13/ 2003 that stated if job training should be carry out in accordance to the requirements of the market and business community and should refer to job competence standards as stated in chapter 1. The provision stated that in carry out the training, it should accordance to several things, such as requirements of the market, business community necessity, and also the job competence standards. However, it should be bear in mind that there are some

[109]Ibid. Part 6A, section 63F (7).

internal procedure in the company that should be followed if employees would like to have some training.

Training could be proposed by employee itself or by company initiatives. If training is proposed by employee itself, all of the expenses should be borne by him or her, unless, he or she would like to propose the training through their unit so the unit leader/ management could carry forward to the learning division, and if it is approved, the employee do not need to pay the expenses by themselves. Second is if the company is having an initiative to held training, then the learning division will notice the selected employee to attend the training, and all of the expenses will automatically be borne by the company. This is similar to the Indonesian Ministry Regulation regarding Competency Based Management Training[110] which set several procedures for approval of training. Further, either by the employee itself or through company initiative, the learning division will support the necessity of the training, such as the training plan, the trainer or coach, the training facilities, the training schedule, as well as the training administration like certificate.

If we look back to the statement bySamGnanakkan[111] that training in ICT companies will cost a lot, not all of the training proposed will be approved by the company. The training proposal which is inline with the company's strategy might be more likely to be approved.

ICT Companies should also look for the importance of personal data protection and data security in the companies. Given the importance of getting data security and data protection right in ICT companies, it is crucial that this is central to ICT companies' strategies, and thus up skilling of relevant employees becomes a priority training objective. And also, in the Indonesian Act of Manpower number 13 year 2003 in Article 158(1i)[112] stated that employee could be dismissed for the reason of unveiling or leaking the company's secrets, this include of personal data or company data that being kept in the company. Therefore, the awareness of the importance of data security and data protection in the workplace is crucial in ICT companies to avoid

---

[110] Indonesian Ministry Regulation 8/2014 regarding Competency Based Management Training, Article 6 (2).
[111] Ibid. (n 15).
[112] Ibid. (n 39), Article 158(1i).

termination of the employee and data breach in the company.

This thesis examines Indonesian ICT companies' perspectives on the implementation of cloud computing. It is important for ICT companies to aware and have an adequate skill in cloud computing, both technological[113] such as software and hardware, and legal[114] such as data security and protection. Not all the employees will be able to understand the technological aspect, however, it is important for all ICT companies to be aware to the legal aspects, especially related to data security and data protection. That is one of the reasons that policy makers should make sure that the ICT employees have full understanding of data security and data protection, as stated in The International Standards Organisation and the International Electrotechnical Commission (ISO/IEC) 27001[115] clause as a guidance for ICT companies to make sure that they have already establish, review and maintain their security systems.

ISO/IEC 27001 is guidance in data security in Indonesia during the implementation period of the new regulations in Information Security Management System (ISMS) and Protection of Personal Data in the Electronic System. ICT companies use ISO/IEC 27001 to prevent crime that might occur in the workplace, and to update the awareness of the employees related to the data security and data protection. The knowledge of the employees is expected to stop them from committing a cybercrime. Kizza[116] explained that cybercrime is an illegal act involving a computer system as an object, a tool to commit a crime, or an evidence of a crime, and further stated that employees might have great potential to become a cybercriminal since they have the authority to access the system; most of the crimes in the technology and telecommunication sector were committed by the employees themselves. With this potential for cybercrime from inside the company, it is necessary for the policy makers in the companies to make sure that all of their employees are aware of the data security and data protection. ICT employees are the most likely to commit crime that involves data security and personal data. They can easily commit a data breach by using the authority that they have.

---

[113]Ibid. (n 54).
[114]Ibid. (n 54).
[115]Alan Calder, *ISO27001* (IT Governance Publishing 2013).
[116]Ibid. (n 37).

Annex A7 ISO/IEC 27001[117] states that companies should offer training on information security risk during the induction of new staff, on-the-job-training, or annually.[118] Training can help employees to be aware of potentials that occur from the implementation of technology in the workplace, and to improve the skill and capability of employees.[119] Through training, employees can prove themselves that they are capable and worthy to stay in the company, since they have the capacity and skill required. Policy makers should realise that educating employees is part of a company's work to support its business strategy.[120]

1.4 Chapter Summary

Cloud computing has brought significant changes in the ICT industry and to the workplace environment. With the rapid development in technology, ICT companies should make sure that their employees are also prepared for the implementation of new technology. There are some aspects that companies, especially policy makers, should be aware of.

Cloud computing is not merely related to technological aspects such as the software and hardware of the systems, but also there are legal aspects that should be known by all employees, such as data security and data protection. Since the Indonesian regulations are relatively new, policy makers should make sure that the ICT employees already know and perform all the obligations related to the legal aspect in cloud computing. This is to ensure that ICT companies and their employees comply with the new regulations, comply with policy related to data security and personal data protection, avoid cybercrime being committed by ICT employees and the potential violation of law by ICT companies.

It is important for the Indonesian government to make sure that it supports the development of technology by making sure that the regulations accommodate the development of technology. It also needsto make sure that business players are aware of and comply with the regulations related to the development of technology. One of

---

[117]Ibid. (n 115).
[118]Ibid. (n 115).
[119]Joanna M Sullivan, *Creating Employee Champions* (Do Sustainability 2014).
[120]Ibid.

the solutions that can be offered by government is to make sure that regulations support the continuous learning process for employees. This is why legal reform is essential to achieve the compliance with regulation of the development of technology and business.

It is unnecessary for all employees to have in-depth knowledge of the technological aspects in cloud computing, but they must perform all the obligations in the regulations. Policy makers should make sure that they include the employees' skill improvement aspect in policy-making, to make sure that the company strategy is in line with the employees' skill development and to ensure that employees are aware of their obligations on data security and data protection. This is important since ICT employees have access to the data on themselves, the company's data, and customers' data.

Improving employees' skill can be achieved through training. Even if there are some obstacles in performing training, it does not mean that employees might refuse the implementation of new technology. Employees should be active to achieve the standard that is required in the field that involves new technology. Lack of opportunity in training should not be an obstacle for employees to develop themselves. Employees should be able to enhance themselves in the workplace to be in line with the companies' strategy. Policy makers should be able to encourage all employees to participate in the implementation of new technology.

Chapter 2. Literature Review

2.1 Introduction

Technology has brought fundamental changes for ICT employees' skills[121] and technology is expected to support the development of Indonesia's economy. However, the implementation of technology itself has raised several legal issues, whether related to the existence of the technology itself, the implementation of the technology or the readiness of the people to implement the technology.[122]

This thesis will discuss the implementation of cloud computing in the workplace. It will reveal an in-depth research on how cloud computing is implented in the workplace. This thesis will elaborate the issues of data security, data protection, as well as data controller and data processor. The concerns in emphasizing those areas are because it related to the ICT companies as the researcher is the employee of the ICT companies, and second is because it related to the responsibility of the ICT employees to provide themselves with sufficient knowledge of the latest technology and its implication. The fast shift of technology has become a must for all employees to be aware of the changes, especially for the ICT employees. Employees have the ethical responsibility to support the government by performing the clause in the Ministry Regulation 8/2014 that states if the training in the company is to make sure that employees meet the Indonesian working standard competence, special standard or international standard. Furthermore, if we look into Indonesian Act Number 13 of 2003 in Article 1(9), job training is an activity of providing workers or potential workers to meet the grade and qualifications for a position.

Therefore, to support the successful of the implementation of regulation in the company, employees need also to have the awareness and eagerness to uplift themselves with sufficient skill and knowledge. It is obligated by the regulation for employers to offer training, even though employees are not legally be required to undertake the training or be sacked for refusing to accept training opportunity, it is ethically responsibility for employee to support the implementation of regulation in

[121]Ibid. (n 1).
[122]Ibid. (n 1).

the company by supporting the company's strategic scenario (CSS) by uplifting themselves with sufficient skill and knowledge.

The development of technology in Indonesia has grown significantly, indicated through the growth of the ICT providers.[123] The EU-Indonesia Business Network (EIBN)[124] states that social networking has increased rapidly in Indonesia. EIBN,[125] is a partnership project that initiated and co-funded by the European Union which launched in 2013 between five European bilateral chambers of commerce in Indonesia and two counterparts in Europe to promote potential trade and investment of Indonesia. On the report, it states that Indonesia, with the 4th largest number of Facebook users in the world in 2013, a growth of internet users from 40 million in 2011 to 175 million in 2016, and the growth of data connection subscribers from 52 million in 2011 to 167 million in 2016, shows that the ICT industry in Indonesia is an attractive market sector. Telecommunications has become a strategic industry,[126] particularly finance IT, cloud computing, e-commerce and e-logistics. To support the strategic business in the ICT industry, it is necessary for the Indonesian government to provide adequate technological and ICT regulations for the implementation of technology in Indonesia, as it is important to prepare the Indonesian citizensfor the development of information technology in the country.

There are a number of studies related to cloud computing, mostly focused on the technical context, for example standard in cloud computing,[127] innovation,[128] jurisdiction and transferring data in the EU,[129] privacy and control of data,[130] data

---

[123]Bruce Wardhaugh, 'Developing Regimes and Mobile Telecoms Regulation in the Twenty-First Century: Who Makes the Call?' (2015) 6 European Journal of Law and Technology (EJLT) <http://ejlt.org/article/view/402/579> accessed 8 June 2016.
[124]'Your Gateway to Indonesia' (*EIBN (EU Indonesia Business Network)*, 2015) <http://www.eibn.org/upload/EIBN_presentations_for_companies_2015_small.pdf> accessed 11 February 2017.
[125]Ibid. (n 80).
[126] Walden I and Angel J, *Telecommunications Law and Regulation* (Oxford University Press 2005).
[127]Ibid. (n 74).
[128]Primavera Filippi and Luca Belli, 'Law of The Cloud V Law of the Land: Challenges and Opportunities for Innovation' (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/156/249> accessed 5 October 2015.
[129]Alessandro Mantelero, 'Cloud Computing, Trans-Border Data Flows and The European Directive 95/46/EC: Applicable Law and Task Distribution' (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/96/254> accessed 5 October 2015.
[130]Ibid. (n 54);
Konstantinos Stylianou, Jamila Venturini and Nicolo Zingales, 'Protecting User Privacy in The Cloud:

protection[131] and contract.[132] Leimbach et al.[133] stated that legal uncertainty and competitiveness in industry have become challenges in cloud computing. He emphasised that legal aspect like data protection, data security, choice of law and economic aspects are important, but that the human capital aspect should also be an important consideration to the emerging of cloud computing sector. Defining the role and responsibility of actors in cloud computing is also vital in the implementation of cloud computing.'The governance of cloud is not only about legal framework, but also about their enforceability'.[134] Hence, to balance the legal framework and the enforceability in the company, there should be adequate awareness of cloud computing,[135] especially for the policy makers. As this will reflect on how they decide the internal policy for the employees and for the business as well.

Data security and protection, and data controller and data processor are important in cloud computing.[136] Therefore, this chapter will focus on the cloud computing legal framework of data security, data protection, data controller and data processor by reviewing the regulations and policy of Indonesia using the European Union, and United Kingdom policy and regulations. These aspects were chosen because, by strengthening those legal frameworks, Indonesia will have protection recognition from the United Kingdom and European Union. As the EU and UK have already implemented regulation through the Directive 95/46/EC[137]and the European Union General Data Protection Regulation (GDPR),[138] EU and UK regulations could be a guide for the Indonesian government in the implementation of data protection and data security.

Recently, the Indonesian government has promulgated the new Regulation of the

---

An Analysis of Terms of Service' (2015) 6 European Journal of Law and Technology <http://ejlt.org/article/view/462/594> accessed 5 August 2016.
[131]Ibid. (n 50), S.K. Chaulya and G.M. Prasad.
[132]Clarice Castro, Chris Reed and Ruy Queiroz, 'On the Applicability of the Common European Sales Law to Some Models of Cloud Computing Services' (2013) 4 European Journal of Law and Technology <http://ejlt.org/article/view/186/409> accessed 5 August 2016.
[133]Ibid. (n 60).
[134]Ibid. (n 60).
[135] Richard Kemp, 'Legal Aspects of Cloud Security' (2018) 34 Computer Law & Security Review.
[136] Paul de Hert, Vagelis Papakonstantinou and Irene Kamara, 'The Cloud Computing Standard ISO/IEC 27018 Through the Lens of The EU Legislation on Data Protection' (2016) 32 Computer Law & Security Review.
[137]Ibid. (n 25).
[138]Ibid. (n 26).

Minister of Communication and Informatics in 2016 related to Information Security Management System (ISMS) and Protection of Personal Data in the Electronic System. Those Ministry regulations are the implementation of the Electronic Information and Transaction Law 11/2008 and the Government Regulation related to Implementation of Electronic System and Transaction 82/2012. The Indonesian governmentis optimistic that these regulations could cope with the protection that required in the implementation of cloud computing.

In addition to these, it is necessary for the Indonesian government to put some considerations related to data control and data processing, especially with the growth of ICT providers in Indonesia.[139] They should be able to specify whether they act as a data controller or data processor. This is important for ICT companies, since the specification will lead to the responsibility and obligation that they will carry as cloud providers. In cloud computing, data could be held anywhere. Therefore, it is necessary to have regulations to determine responsibility in a cloud computing service.

2.2 Legal Aspects of Data Protection and Data Security Law Reform in the Cloud Computing Industry

Technology has shifted the behaviour of ICT users. It gives more freedom to use, contribute, provide and control the data over the storage and software facilities.[140] They tend to be online and active in their social media.[141] People find it easier to get and share any information that they need and have through technology. For ICT providers, these phenomena have given them a new prospective on the business. They have competed to deliver the best service for the customers. The customers' online behaviour has generated a new business for ICT providers to provide the storage to keep and share the data, which is called cloud computing. According to NIST, cloud computing is:

> 'A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers,

[139]Ibid. (n 124).
[140]Charles Oppenheim, *the No-Nonsense Guide to Legal Issues in Web 2.0 And Cloud Computing* (1st edn, Facet 2012).
[141]Misty Blowers, *Evolution Of Cyber Technologies And Operations To 2035* (1st edn, Springer International Publishing 2015).

> storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'.[142]

This definition is use as a reference industry-wide.[143] Therefore, there are networks, servers, storage, applications, and services in cloud computing.[144] This section will elaborate the characteristics, delivery models, deployment models and protection in cloud computing.

2.2.1 An evolving definition of cloud computing

Although NIST's definition is commonly used to define cloud computing, other research has also tried to define it. Vaquero et al.[145] explained that there are more than twenty researchers have tried to define the term, and characterised it as involving user friendliness, virtualisation, internet centricity, variety of resources, automatic adaption, scalability, resource optimisation, pay per use, service of Service Level Agreements (SLAs), and infrastructure of Service Level Agreements (SLAs). Bhatt[146] explained that cloud computing is a package of hardware, software, storage and services that are accessible on a time delivery service. Gartner[147] explained the definition of cloud computing as a style of scalable and elastic IT resources that delivered a service to customer using the internet. Erl[148] defined it as a specialised form of circulation of computing with remotely accessible and measured resources. However, it was McCarthy[149] in the 1960s who first discussed the utility of cloud computing. In 1966, Parkhill[150] expanded the concept by comparing it with the usage of water, natural gas and electricity. The term of usage in computing resources should be treated the same as electricity supply. Cloud computing should be accessible any

---

[142]Ibid. (n 46).
[143]Ibid. (n 45).
[144] Talal H. Noor et al., 'Mobile Cloud Computing: Challenges and Future Research Directions' (2018) 115 Journal of Network and Computer Applications.
[145]Luis M. Vaquero et al., 'A Break in the Clouds' (2008) 39 ACM SIGCOMM Computer Communication Review.
[146]Ibid. (n 47).
[147]David W. Cearley, 'Cloud Computing - Key Initiative Overview' (*Gartner.Inc*, 2010) <https://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_CloudComputing.pdf> accessed 12 February 2015.
[148]Thomas Erl, *'Cloud Computing: Concepts, Technology, & Architecture'* (1st edn, Pearson Education (US) 2013).
[149] Inderveer Chana and Tarandeep Kaur, 'Delivering IT As A Utility- A Systematic Review' (2013) 3 International Journal in Foundations of Computer Science & Technology.
[150]Ibid. (n 50), S.K. Chaulya and G.M. Prasad, S.K. Chaulya and G.M. Prasad

time and only be billed by the usage. Cloud computing then assumed as a comprehensive delivery service through the internet network using hardware and software and is accessible at anytime and paid as used.

Zhang[151] stated that cloud computing is not a new technology, but existing technologies gathered into a new operation business model. Indeed, if we refer to NIST definition, it clearly states that cloud computing is a business model that requiresa network, servers, storage and applications that mould into a service.[152] Therefore, ICT providers with the technology required in cloud system, should find no difficulties in doing business in cloud computing. However, if cloud computing is not a new technology for ICT business, then what distinguishes cloud computing to other business?

If we refer to the definitions above, cloud computing can be assumed to be the use of software and hardware in designated storage through a network that is being delivered by a cloud provider through specific services. The factors that distinguish cloud from other businesses is that, in cloud services, the use in the service is manageable. Referring to the definitions of McCarthy[153] and Parkhill,[154] we only claimed by the use we made in the cloud service. Minimum cost in internet and data storage,[155] accessible applications and pay-per-use service,[156] in other words, cheap, fast, secure and available internet access, have become the key matters for ICT users. The user of a cloud does not need to build the network, or storage, or software and hardware; instead, they can outsource it to the cloud provider.[157] This could save money on the infrastructure and maintenance.

The development of cloud computing is affected by the demand in the market and

---

[151]Qi Zhang, Lu Cheng and Raouf Boutaba, 'Cloud Computing: State-Of-The-Art and Research Challenges' (2010) 1 Journal of Internet Services and Applications.
[152]Ibid. (n 46).
[153]Ibid. (n 149).
[154]Ibid. (n 50), S.K. Chaulya and G.M. Prasad.
[155]Ibid. (n 47).
[156]Richard Hill et al.,*Guide to Cloud Computing* (1st edn, Springer London 2012).
[157]Stefanie Leimeister et al., 'The Business Perspective of Cloud Computing: Actors, Roles and Value Networks', *18th European Conference on Information Systems* (ECIS 2010 Proceedings 2010) <http://aisel.aisnet.org/ecis2010/56> accessed 14 February 2017.

finance fluctuation.[158] The comprehensive new business service in cloud computing then became attractive for the ICT provider to deliver services to meet the market requirements. There are many benefits that users can grasp by deploying cloud computing. Carroll[159] stated that the cost of efficiency, followed by scalability, flexibility, agility, better IT resource and business focus, and green IT data centres, have become a great concern in choosing cloud computing as a new business model. Therefore, to deliver a good performance in cloud computing, cloud providers should be able to guarantee that they have the authority to have the software, hardware, network and storage as a business. Cloud providers should be able to harmonise the necessity between cloud architecture, cloud service, and the implication from implementation cloud computing.

Cloud architecture as has been alluded on the Chapter 1.2,[160] could be distinguished as cloud application (Software as a Service or SaaS), platform (Platform as a Service or PaaS), infrastructure (Infrastructure as a Service or IaaS), and server. Cloud architecture is used to identify types of services to deliver to users, known as cloud delivery models. Each delivery model is characterised by the package of IT resource offered by provider. It guides cloud user to choose the appropriate technology for their business.

Delivery service is important to determine which cloud service protection is suitable for the cloud user. It requires protection in delivering a cloud service, such as data security, data protection and data storage.[161] Commonly, cloud delivery is known for its three basic models, which are infrastructure, platform and software. Providers often have their business model framework in these three technical bases.[162] There are some delivery services that cloud computing could offer, and there are six delivery services that are well-known in the Indonesian ICT business. Those services are:

---

[158] Michael H Hugos and Derek Hulitzky, Business in the Cloud (1st edn, Wiley 2011). .
[159]Mariana Carroll, Alta van der Merwe and Paula Kotze, 'Secure Cloud Computing: Benefits, Risks And Controls' [2011] 2011 Information Security for South Africa.
[160] Yashpalsinh Jadeja and Kirit Modi, 'Cloud Computing - Concepts, Architecture and Challenges' [2012] 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET).
[161]S. Subashini and V. Kavitha, 'A Survey on Security Issues in Service Delivery Models of Cloud Computing' (2011) 34 Journal of Network and Computer Applications.
[162]Ibid. (n 56).

Infrastructure as a service (IaaS)

IaaS is a cloud infrastructure that provides a firm cost saving,[163] because the user does not need to provide or manage the system, storage or network, however, they have a control of those infrastructures.[164] IaaS only provides basic security software.[165]

Platform as a service (PaaS)

PaaS is a cloud service that leverages a complete software service from cloud programming to implementation.[166] It connects hardware and applications.[167] Since PaaS is one layer above IaaS, it is vulnerableto being use by hackers to deliver malware and control it through IaaS application.[168]

Software as a service (SaaS)

SaaS is a network-based access service[169] and delivered over the internet.[170] Cloud users can access and pay for the application based on their requirements.[171] There is paid and free software; however, if cloud users would like to add more security, the pay-software provides more security based on the SLA between user and provider.[172]

Network as a service (NaaS)

NaaS is a service that is a virtualised network over the internet.[173] Users can pay cloud providers if they want to rent the resource.[174] It is a secure, easily installed custom

---

[163]Ibid. (n 159).
[164]Tharam Dillon, Chen Wu and Elisabeth Chang, 'Cloud Computing: Issues And Challenges' [2010] 2010 24th IEEE International Conference on Advanced Information Networking and Applications..
[165]Ibid. (n 59).
[166]Alexander Lenk et al., 'What's Inside the Cloud? An Architectural Map of the Cloud Landscape' [2009] 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing.
[167]Chunye Gong et al., 'The Characteristics of Cloud Computing' [2010] 2010 39th International Conference on Parallel Processing Workshops.
[168]Ibid. (n 156).
[169]Ibid. (n 159).
[170]Michael Armbrust et al., 'A View of Cloud Computing' (2010) 53 Communications of the ACM..
[171]Ibid. (n 56).
[172]Anubhav Jain, Manoj Kumar and Anil Lambha, 'An Overview and Trends In Cloud Computing' [2015] International Journal of Computer Applications..
[173]Sheikh Habib et al., 'Trust as a Facilitator in Cloud Computing: A Survey' (2012) 1 Journal of Cloud Computing: Advances, Systems and Applications..
[174]Rasheed Hussain et al., 'Rethinking Vehicular Communications: Merging VANET with Cloud Computing' [2012] 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings.

routing and multicast protocol, which can be used efficiently and is cost-effective.[175]

Communication as a service (CaaS)

CaaS is an internet-based based voice and data service that delivers Voice over IP, instant messaging and video conferencing as a service.[176] Providers of CaaS has a responsibility to the hardware and software and the quality of service.[177]

Disaster Recovery as a Services

The emergence of disaster recovery as a service is mainly to protect cloud users, especially companies, from a disaster that could lead to IT failure and significant data loss.[178] In cloud computing, data centres play an important role, because they integrate a variety of different systems such as a servers, power supplies and networks.[179] Small faults in data servers can have a huge effect in the system. Disaster recovery planning is important to backup any unexpected disaster. According to McCarthy[180] and Parkhill,[181] data centres play a big role. It is not merely keeping the data of its users, but also how they maintain that data.

Data recovery providers need to provide their staff with a sufficient knowledge and skill to prepare for the disaster and damage and maintain and protect it's the data centre with protections like identifying network system, providing backup hardware, installing software firewalls on the operating system, and socialising an appropriate disaster plan.[182] However, high cost, weak guarantees of data lost and recovery time

---

[175]Paolo Costa et al., 'Naas: Network-As-A-Service In The Cloud', *2nd USENIX Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services* (USENIX 2012) <https://www.usenix.org/conference/hot-ice12/naas-network-service-cloud> accessed 13 February 2016.

[176]Eman M. Mohamed, Hatem S. Abdelkader and Sherif EI-Etriby, 'Enhanced Data Security Model for Cloud Computing', *the 8th International Conference on INFOrmatics and Systems* (2012).

[177]George Suciu et al., 'Cloud Consulting: ERP and Communication Application Integration in Open Source Cloud Systems' [2011] 2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers.

[178]Timothy Wood et al., 'Disaster Recovery As A Cloud Service: Economic Benefits & Deployment Challenges', *2nd USENIX conference on Hot topics in Cloud Computing* (USENIX 2010).

[179]Albert Greenberg et al., 'The Cost Of A Cloud' (2008) 39 ACM SIGCOMM Computer Communication Review.

[180]Ibid. (n 149).

[181]Ibid. (n 50), S.K. Chaulya and G.M. Prasad.

[182]Louis Turnbull et al., 'Improving Service Continuity: IT Disaster Prevention and Mitigation for Data Centers' [2013] Proceedings of the 2nd annual conference on Research in information technology - RIIT '13.

have become problems for existing providers.[183]

Indonesia ICT Companies in this thesis have implemented and marketed Software as a Service (SaaS), Infrastructure as a Service (IaaS), Disaster Recovery as a Service, Platform as a Service (PaaS), as well as Public cloud and Private Cloud.

These models of services have highly connected to the data protection and data security. Different layer of services has generated the importance of awareness in data security and data protection in ICT companies[184] and failure to perform prediction, sensitivity and accuracy for a distributed computing system and the component in each service might affect performance of the companies.[185] If we look especially in Disaster Recovery as a Service, it would required high protection on data security and personal data, since data that being kept in the premises have to be backed up and companies have to make sure that data are all available and well protected in the premises, as well as cost control, data duplication, and security issues.[186]

Those delivery services offered by cloud provider have helped cloud users to understand the benefits they will receive from the cloud service. Security systems of cloud provider have become the base requirement. Cloud providers have to make sure that they protect security in every aspect in cloud computing. The cloud user is then expected to choose a service based on what they require. The use of cloud computing for users could be clustered into ownership, size and access for customer delivery services. Users need to know what type of cloud service that they need. Generally, as defined by NIST, there are four categorises in cloud deployment model. They are:

Public cloud

In public cloud, the infrastructure over the internet[187] is available for the public or a large industry, however, this model would probably not be applicable for those who

---

[183]Ibid. (n 178).
[184]Flora Amato and others, 'Improving Security In Cloud By Formal Modeling Of Iaas Resources' (2018) 87 Future Generation Computer Systems.
[185]Bashir Mohammed and others, 'Failure Analysis Modelling In An Infrastructure As A Service (Iaas) Environment' (2018) 340 Electronic Notes in Theoretical Computer Science.
[186]Júlio Mendonça and others, 'Disaster Recovery Solutions For IT Systems: A Systematic Mapping Study' (2019) 149 Journal of Systems and Software.
[187]Aiden E Williams, *Public Cloud Computing* (1st edn, Nova Science Publishers 2012).

need wide-ranging security and privacy.[188] Business, academic and government organisations have owned, managed and operated them.[189]

Private cloud

In private cloud, the infrastructure is intended for one single organisation.[190] They have total authority over management, security, maintenance and use.[191] It accessible only for users who have access to the system as an intranet.[192]

Community cloud

Community clouds exist because of the idea of Digital Ecosystems research.[193] It stands between a public and private cloud.[194] The infrastructure resources are shared for two or more of the community members. The cost can be cheaper than a private cloud, but higher than a public cloud. The user can distribute the maintenance of the cloud to a cloud provider.

Hybrid cloud

Hybrid cloud is a combination of infrastructure to supplement within clouds (private, public, or community) to handle workload fluctuations.[195] However, there are some issues related to the standardisation and interoperability on the transferring process.[196]

To understand the requirement in cloud infrastructure can help the cloud user to obtain the benefits of the cloud service. The user might be able to choose to have their own cloud infrastructure or share it; all depending on the requirements of the user. However, it is necessary for cloud users to understand the consequence in choosing a

---

[188]Rob Zanella and Sumner Blount, *Cloud Security and Governance: Who's on Your Cloud?* (1st edn, IT Governance Ltd 2010).
[189]Dan C. Marinescu, *Cloud Computing: Theory and Practice* (1st edn, Morgan Kaufmann Publishers 2013).
[190]Z Lei et al., 'Comparison of Several Cloud Computing Platforms', *Second International Symposium on Information Science and Engineering* (2009).
[191]Ibid. (n 54).
[192]Ibid. (n 156).
[193]Gerard Briscoe and Alexandros Marinos, 'Digital Ecosystems in the Clouds: Towards Community Cloud Computing', *3rd IEEE International Conference on Digital Ecosystems and Technologies* (Institute of Electrical and Electronics Engineers (IEEE) 2009).
[194]Sumit Goyal, 'Public Vs Private Vs Hybrid Vs Community - Cloud Computing: A Critical Review' (2014) 6 International Journal of Computer Network and Information Security.
[195]Ibid. (n 188).
[196]Ibid. (n 160).

cloud service. They need to look carefully at services offered by cloud providers, since they might be unaware of the exact location of their data which being kept by the cloud provider.[197]

Cloud computing has transformed the behaviour of the user in the IT industry.[198] Cloud users should know and understand their rights and obligations when choosing cloud services. Aside from the benefits, users also need to know the potential risks.[199] Beside the technological infrastructure issues, data security and privacy[200] have become the users' main concerns.

Cloud computing has offered a lot of advantages in its utilities. Recently, it has also been proven to support the energy efficiency by using data centre.[201] However, to support the development of technology in cloud computing, it is necessary for the user to be aware to the impact of the legal aspects in using cloud computing. Cloud computing is always related to data security and privacy of the data stored on the premises.[202] The new development in cloud service such as containers, acceleration

---

[197] Nalini Subramanian and Andrews Jeyaraj, 'Recent Security Challenges in Cloud Computing' (2018) 71 Computers & Electrical Engineering.
[198]Xun Xu, 'From Cloud Computing To Cloud Manufacturing' (2012) 28 Robotics and Computer-Integrated Manufacturing.
[199]Christos Stergiou et al., 'Secure Integration of IoT and Cloud Computing' (2018) 78 Future Generation Computer Systems.
[200]Ibid. (n 156);
Ibid. (n 157);
Nelson Gonzalez et al., 'A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing' (2012) 1 Journal of Cloud Computing: Advances, Systems and Applications;
Ibid. (n 160);
Erdal Cayirci et al., 'A Risk Assessment Model for Selecting Cloud Service Providers' (2016) 5 Journal of Cloud Computing;
Mladen A. Vouk, 'Cloud Computing: Issues, Research and Implementations' (2008) 16 Journal of Computing and Information Technology;
Mark D. Ryan, 'Cloud Computing Privacy Concerns on Our Doorstep' (2011) 54 Communications of the ACM;
Lori M. Kaufman, 'Data Security in the World of Cloud Computing' (2009) 7 IEEE Security & Privacy Magazine;
Ibid. (n 61);
Ibid. (n 74);
Ibid. (n 73);
Ibid. (n 130), Konstantinos Stylianou, Jamila Venturini and Nicolo Zingales.
[201]Ali Vafamehr and Mohammad E. Khodayar, 'Energy-Aware Cloud Computing' (2018) 31 the Electricity Journal.
[202]P. Ravi Kumar, P. Herbert Raj and P. Jelciana, 'Exploring Data Security Issues and Solutions in Cloud Computing' (2018) 125 Procedia Computer Science.

and function[203] requires ICT companies to always review to the compliance of policies and regulationson the data security and data protection.[204] The development of cloud computing will require a lot of useof data centre and devices anda network to gather and exchange data.[205] Therefore, it is necessary for ICT companies to make sure that they have provide adequate protection related to data security and personal data protection to support the development of technology, especially in cloud computing, such as for supporting the face feature data[206] or finger vein images.[207]

Cloud computing will develop rapidly in the future and it will require readiness not only on the technological aspects, but also related to the legal aspect.[208] Varghese and Buyya[209] explained that some developments will create a trends and directions in changing infrastructure, impact areas, emerging architectures and directions. Cloud computing will emerge rapidly to meet user demand.[210] Those areas of trends and directions will involve a lot of data use, and so legal issues such as data security and protection are being challenged.[211] Along with the development of cloud computing, some studies[212] have revealed that security and privacy issues have become the

---

[203]Blesson Varghese and Rajkumar Buyya, 'Next Generation Cloud Computing: New Trends and Research Directions' (2018) 79 Future Generation Computer Systems.
[204]Ibid. (n 200).
[205] Ibid. (n 199).
[206]Pengfei Hu et al., 'A Unified Face Identification and Resolution Scheme Using Cloud Computing in Internet of Things' (2018) 81 Future Generation Computer Systems.
[207]Zhendong Wu et al., 'Generating Stable Biometric Keys for Flexible Cloud Computing Authentication Using Finger Vein' (2018) 433-434 Information Sciences.
[208]Azzedine Boukerche and Robson E. De Grande, 'Vehicular Cloud Computing: Architectures, Applications, and Mobility' (2018) 135 Computer Networks.
[209]Ibid. (n 203).
[210]Ibid. (n 206).
[211]Sreeja Cherillath Sukumaran and Misbahuddin Mohammed, 'PCR and Bio-Signature for Data Confidentiality and Integrity in Mobile Cloud Computing' [2018] Journal of King Saud University - Computer and Information Sciences.
[212]Nesrine Kaaniche and Maryline Laurent, 'Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms' (2017) 111 Computer Communications,
Ibid. (n 201);
Duha Alsmadi and Victor Prybutok, 'Sharing and Storage Behaviour via Cloud Computing: Security and Privacy in Research and Practice' (2018) 85 Computers in Human Behaviour;
Ibid. (n 199);
Gregory Levitin, Liudong Xing and Yuanshun Dai, 'Co-Residence Based Data Vulnerability Vs. Security in Cloud Computing System with Random Server Assignment' (2018) 267 European Journal of Operational Research;
Ashish Singh and Kakali Chatterjee, 'Cloud Security Issues and Challenges: A Survey' (2017) 79 Journal of Network and Computer Applications;
Gururaj Ramachandra, Mohsin Iftikhar and Farrukh Aslam Khan, 'A Comprehensive Survey on Security in Cloud Computing' (2017) 110 Procedia Computer Science;

biggest concern in cloud computing service and have found some solutions to the issues.

2.2.2 Principles of data security and data protection

Cloud providers should be certain that they protect their customer not only related to the internet content, but also the IT infrastructure and application. Blount and Zanella[213] stated that there are three types of security in the cloud, security to the cloud, for the cloud, and from the cloud. Security is captured from the cloud service and deployment models. Therefore, cloud providers should confirm that security in the cloud should cover infrastructure, applications and data, software, hardware, and servers.

Carroll[214] explained that cloud security consists of data privacy, data control, availability of data and service, data integrity, and data encryption. Cloud users need to be assured that they have appropriate protection for their data, the network, infrastructure, application and storage. Robinson[215] defined security as the confidentiality and availability of data or information, including encryption, and privacy as an expression through legal and non-legal norms to protect the right to personal or private life.

NIST stated that cloud computing:

> '…is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'.[216]

The definition has described that cloud computing should be able to provide a ubiquitous and on-demand network access to a shared computing resource. It means that cloud computing providers should be able to make sure that there will be no data

---

Syed Asad Hussain et al., 'Multilevel Classification of Security Concerns in Cloud Computing' (2017) 13 Applied Computing and Informatics;
Saurabh Singh, Young-Sik Jeong and Jong Hyuk Park, 'A Survey on Cloud Computing Security: Issues, Threats, And Solutions' (2016) 75 Journal of Network and Computer Applications.

[213]Ibid. (n 188).
[214]Ibid. (n 159).
[215]Neil Robinson, *The Cloud* (1st edn, Rand 2011).
[216]Ibid. (n 46).

leakage during the process of data transfer. Therefore, cloud computing providers should employ additional security measures to make sure that data is safe on the premises and there are no data breaches during the process.[217] This is data security.[218] In data storage, the customer's data is kept in a remote server and the customer has limited access over the controlling and monitoring of the storage lifecycle of the cloud provider.[219] The cloud provider should be able to make sure that they protect the data, they have a data recovery process, and data is protected from malicious tampering.[220] The shared computing resource might also be a trigger to data integrity loss and data privacy loss.[221] Therefore, comprehension of data security is necessary for the cloud provider to protect the confidential data of their customer,[222] to comply with regulation and policy related to data security, to process and control the data kept, and to control people who have access to it.[223]

Mostly, data security concerns in cloud computing are related to data segregation and protection and data leak prevention.[224] Data security has been continuously studied to fulfil the proper protection in cloud computing.[225] Most of the consideration in data security is how the cloud computing provider protects data, especially personal data. This is important since in the personal data, the data subject can be identified or identifiable.[226]

In 1981, the Convention for the Protection of Individual with regard to Automatic

---

[217]Ibid. (n 201).
[218]Ibid. (n 212), Gregory Levitin, Liudong Xing and Yuanshun Dai.
[219]Rongzhi Wang, 'Research on Data Security Technology Based on Cloud Storage' (2017) 174 Procedia Engineering.
[220]Ibid.
[221]Ibid. (n 212).
[222] Hui Na Chua et al., 'Impact of Employees' Demographic Characteristics on The Awareness and Compliance of Information Security Policy in Organisations' (2018) 35 Telematics and Informatics.
[223] Chen Zhong et al., 'A Cyber Security Data Triage Operation Retrieval System' (2018) 76 Computers & Security.
[224] R. Velumadhava Rao and K. Selvamani, 'Data Security Challenges and Its Solutions in Cloud Computing' (2015) 48 Procedia Computer Science.
[225] Qin Liu et al., 'Preface: Security and Privacy in Big Data Clouds' (2017) 72 Future Generation Computer Systems; Valentina Casola et al., 'Monitoring Data Security in The Cloud: A Security SLA-Based Approach' [2018] Security and Resilience in Intelligent Data-Centric Systems and Communication Networks; Riswana Shaikh and M. Sasikumar, 'Data Classification for Achieving Security in Cloud Computing' (2015) 45 Procedia Computer Science.
[226]Ibid. (n 26), Article 4(1).

Processing of Personal Data (ETS No. 108)[227] was ratified. It is an open convention, to which any country can apply to consent to this convention, including Indonesia as an observer state.[228] Convention 108 is the only legally binding international instrument in the data protection for states that have ratified it.[229] It discuss on how to protect individuals against misuses on the processing of personal data, and how to regulate personal data protection in transborder territorial. Until recent, there are total of 51 countries that become parties to Convention 108, include of 47 countries of the Council of Europe, Uruguay, Mauritius, Senegal and Tunisia. Even though Indonesia as an observer state has substantial populations, in the regards of the lack of data privacy, Indonesia have limited global influence.[230] Convention 108 has the most signatories, and arguably influence, to date.

In 24 October 1995, the EU published Directive 95/46/EC[231] which specifies the lawfulness in processing personal data and the rights of the people on the process and appoints a representative to monitor implementation. In 2002, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)[232] was produced. This directive was concerning with the terms not covered in Directive 95/46/EC, due to the advances in digital technology. The directive was amended by Directive 2009/136/ECof the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on

---

[227] European Treaty Series - No. 108, Article 4-8.
[228]'Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data' (*Rm.coe.int*, 2019) <https://rm.coe.int/observers-state-of-play-and-admission-criteria/16808fdc4d> accessed 10 April 2019.
[229]*Handbook On European Data Protection Law* (European Union Agency for Fundamental Rights and Council of Europe 2018).
[230] G. Greenleaf, 'The Influence Of European Data Privacy Standards Outside Europe: Implications For Globalization Of Convention 108' (2012) 2 International Data Privacy Law.
[231]Ibid. (n 25).
[232]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)

Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws[233] which established a legal framework for the breach of personal data.

As the newest regulation, GDPR, has only recognised one 'third' country (Japan) as providing adequate level protection (it has rolled over existing adequacy decisions made under Directive 95/46/EC pending review in due course). However, the extra-territorial applicability provision in Art 3[234] means it has the potential to become globally influential. Its goal to strengthen protection in personal data and data security has inspired Indonesia to have a good model of protection to follow; moreover, Indonesia has strong and growing economic ties with the EU, and if Indonesian companies do not comply with GDPR standards then personal data transfers between the two will not be effectuated lawfully (unless individual companies use mechanisms in Art 46 to effect transfers).

If the Indonesian government envisages greater economic ties/ links with the EU/ European Economic Area (EEA) countries then it should consider applying for an adequacy decision (either a general/ partial adequacy decision), and this would be more cost effective than requiring individual companies to rely on Binding Corporate Rules/ Standards Contractual Clauses. In Binding Corporate Rules, companies will have to make more effort to meet the requirement in EU/ EEA. In order to get the approval, Binding Corporate Rules must fulfil some requirement, such as must be legally binding, apply to all concerned member of the international organization, clear for data subjects to exercise their data subject rights, mention specific information with regards to the organization and processing.[235] Those efforts will require a long

---

[233]Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications); Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws (the Regulation on Consumer Protection Cooperation)

[234] Ibid. (n 26) Art 3(3)

[235] Ibid. (n 26), Art 47 (2)

process of the approval. To have an essential equivalent level of data protection and data security will easier the Indonesian government to support the economic ties in business and partnership between EU and Indonesia as well as European Economic Area (EEA) and Indonesia.

An example of the importance to have an equivalent level of data protection and data security is reflected when the ICT companies would like to expand its subsidiaries or would like to send its employees to have a knowledge through Global Talent Program (GTP). Telkom has a program for top talent employees in the company to become great leaders and great people to support the company's business goals through the experience of of international assignments and certifications. The international assignments countries are including some of EU countries.[236] Indonesian employees are placed in the international companies to learn and do a benchmarking related to the business strategy in international company, further; Telkom's employees are expected to make a partnership with those companies. Telkom's employees might have a partnership with EU's company in cloud computing business, they should be aware and understand to any legal consequences if there is data that should be protected and what is not, what kind of data that could be include in GDPR that should be protected. And as a potential business in data processing or data controller, Indonesia ICT Companies have to fulfil the requirement of equivalent level of data protection and data security in EU. This is the reason that Indonesian cloud computing company currently ensure GDPR compliance in the respect of personal data and data security. This has become the thesis consideration and rationale for comparing Indonesian law with the GDPR. Another rationale for adopting the highest (GDPR) standards and applying those rules in all locations of the GTP is because Telkom has to comply with more than one set of data protection and data security; therefore, it will become a burdensome for the company to have to comply with more than one set of data protection and data security in all locations.

In 2013, European Commission released a Report[237] based on the several considerations (see Appendix 1), underlining a number of concerns related to access

[236] 'Telkom Corporate University Learning Journey' (Telkom Corporate University 2017).
[237] European Report 2013/2063(INI).

to data, cloud computing, best practice in cloud computing, data protection specifically related to data storage, data control and data processing, contracts and certification of cloud services. The EU considers that protection on cloud computing is important since people are using the cloud without knowing it.[238] There should be sufficient protection and policy on the use of the cloud. The report emphasises the importance of data protection in all aspects. Cloud users' data can be stored anywhere; therefore, it is necessary for cloud providers to protect the data and, to have legal certainty, the cloud provider should state it on the contract. The case of *European Court of Justice: C-362/14-Schrems* on the transferring of personal data from Facebook Ireland to a third country has given an insight into how the EU protects the personal data of its citizens. The EU affirms that the third country should have an adequate and equivalent data protection in its domestic law or international commitments.[239]

In 2016, there were three important regulation and directives published by EU in relation to cloud computing. Those are Regulation 2016/679,[240] Directive 2016/680,[241] and Directive 2016/1148.[242] Regulation 2016/679 strengthens the protection of citizens' right on personal data and the rules for business, and emphasised the rules for data controllers and data processors. Directive 2016/680 set out how to treat data protection by the competent authorities, and Directive 2016/1148 set out how to achieve a maximum level of security of network and information systems across the European Union.

The EU has very strict rules on data security and data protection, especially for data that is processed and stored outside EU territory. This is because EU has released its initiative that focuses on the development of an open science cloud and data infrastructure under the Digital Single Market Strategy.[243] Those initiatives focused on

---

[238]'European Commission - Press Release - Unleashing the Potential of Cloud Computing in Europe - What Is It and What Does It Mean for Me?' (*Europa.eu*, 2012) <http://europa.eu/rapid/press-release_MEMO-12-713_en.htm> accessed 23 July 2016.
[239]Ibid. (n 25), Article 25 (6).
[240]Ibid. (n 26).
[241]Ibid. (n 27).
[242]Ibid. (n 28).
[243]'European Egovernment Action Plan 2016-2020 - Digital Single Market - European Commission' (*European Commission*, 2016) <https://ec.europa.eu/digital-single-market/en/node/81744> accessed 20

how the cloud can support the implementation of data sharing and the security of data storage in the EU. The infrastructures consist of network, computing (distributed and high-performance) infrastructure, data infrastructure, and virtual research communities.[244] Furthermore, to support the development of cloud infrastructure, the EU has established the European Cloud Partnership (ECP)[245] which is made up of high-level procurement officers of European public bodies and the ICT industry. ECP will help to identify the needs of the industry players in light of the development of the cloud computing industry. Cloud computing as a part of pillar of the digital single market strategy in EU has given a space for providers to expand their business.[246]

In March 2016, the EU has established the European Cloud Initiative (ECI) as to address how cloud can be use and applicable in all sectors of economy in Europe.[247] This initiative includes solutions in certification, networks, information security, personal data protection, SLA, interoperability and data portability, contracts, prospect of cloud service, and the establishment of European Research Open Science Cloud. The background to this initiative is the benefits of using cloud computing that can promote the development of new business between 2015 and 2020. The initiative's purpose is to provide European industry with data storage infrastructure and management, data connectivity and high performance computers to process data to facilitate EU members in big data era.

The European Telecommunications Standards Institute (ETSI)[248] has also launched a strategy to support the implementation of cloud computing in all economic sectors. With the launch of the eGovernment Action Plan 2016-2020,[249] it is expected that it will maximise the use of technology in public administration, the digital internal market, and public and business services. Cloud computing has become important for

---

July 2016.
[244]Ibid.
[245]Ibid. (n 243).
[246]Ibid. (n 243).
[247]'Cloud Computing Strategy - Digital Single Market - European Commission' (*EU Commission*, 2016) <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy> accessed 20 July 2016.
[248]'Cloud Standards Coordination Final Report' (*European Telecommunications Standards Institute*, 2013) <http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF> accessed 20 July 2016.
[249]Ibid. (n 243).

EU economic development and the Commission has established a unit of Cloud and Software (Unit E.2) under the Future Directorate (Directorate E), under the Directorate General for Communication Networks, Content and Technology.[250] This unit is responsible for the development and implementation of the cloud, including certification, contracts, standardisation, regulation and self-regulation of cloud services, and all cloud based technology environments.

EU support for developing countries such as Indonesia has been recognised by its contribution of more than €500 million in development assistance over the last ten years. In the Blue Book,[251] it is stated that the EU and Indonesia will work together to counter today's global challenges through one of the EU priorities in strengthening the field of science and technology. With the negotiation of the Comprehensive Economic Partnership Agreement, the EU and Indonesia agreed to provide the framework of the agreement.[252] Therefore, it is necessary for both the EU and Indonesia to prepare themselves for the requirements of this partnership, including readiness in the legal environment.

In terms of technology, especially in the cloud, Indonesia did not have a specific regulation on Information Security Management System until the Ministry of Communication and Information Technology regulated it in April 2016. Before the Ministerial Regulation was promulgated, ICT companies used the guidance on the protection of data security in ISO/IEC 27001. GR 82/2012 regarding the Implementation of Electronic Systems and Transactions[253] stated that Electronic System Operators should guarantee the availability and the protection of information security. Information security is defined in Indonesian Ministry Regulation 4/2016 regarding Information Security Management Systems.

The provision of Indonesian Ministry Regulation 4/2016 has states that:

> 'Electronic System Operator which conduct a strategic electronic system should apply the SNI ISO/IEC 27001 standard and safeguard provision

---

[250]'Who We Are - Digital Single Market - European Commission' (*European Commission*, 2016) <https://ec.europa.eu/digital-single-market/en/who-we-are-dg-connect> accessed 20 July 2016.
[251]Ibid. (n 98).
[252]Ibid. (n 98).
[253] Indonesian Government Regulation 82/2012 regarding the Implementation of Electronic Systems and Transactions, Article 12.

established by the Supervisory and Regulatory Agencies'.[254]

The Regulation stated that information security is a responsibility of the electronic system operator to make sure there will be adequate protection of confidentiality, integrity and availability of information, in the relation to personal data, using a risk management system. Electronic system operator is defined as:

> 'Any Person, state agency, Business Entity, and community that provide, manage, and/or operate Electronic System individually or jointly to Electronic System User for its interest or other party's interest'.[255]

The ICT companies in this thesis can be classified as electronic system operators. Therefore, it is the responsibility of ICT companies to make sure that they comply with the regulation and to make sure that all the employees are aware of and implement the provisions of the regulation.

The EU has also stated that it is important for companies in the telecommunication sectors to make sure that they have appropriate procedures in delivering their services. It is stated in EU Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning The Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector[256] that:

> 'The provider of a publicly available telecommunications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented'.

If we look at the EU provision, the provider of telecommunication services should ensure a level of security appropriate to the risk. This is to make sure that they protect personal data, and in particular the right to privacy.EU has emphasised that it is important for telecommunication providers to ensure the protection of data security and personal data.

---

[254]Ibid. (n 10), Article 7.
[255]Ibid. (n 10), Article 1(2).
[256] EU Directive 97/66/EC concerning The Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, Article 4(1).

Awarenessof the importance of data security in Indonesia has been triggered by the level of cybercrime, which has risen massively since 2003.[257] Clearly, readiness of the infrastructure, regulation or policy and human resource is needed to support the development of information technology in Indonesia. Therefore, in 2007, Indonesia's Ministry of Communication and Informatics released the Ministry Regulation regarding the Securing The Making Use of Internet Protocol Based Telecommunication Network [258] that designated Indonesia's Security Incident Response Team on Internet and Infrastructure/Coordination Center (Id-SIRTII/CC) to secure the use of the internet in Indonesia. The Id-SIRTII/CC, revised by Ministry Regulation 2010 regarding Second Amendment to the Decree of the Minister of Communication and Information Technology Number 26/Per/M.Kominfo/5/2007 on Securing The Making Use of Internet Protocol Based Telecommunication Network,[259] makes sure the security of the internet in Indonesia and the consistency of its designation. The team also should identify any internet disruption. The team should be able to make sure that ICT providers provide an appropriate internet system for customers in Indonesia, including making sure that there is adequate data security.

A 2016 survey[260] by the Indonesia Internet Service Provider Association stated that the number of Indonesian internet users is increasing. The survey revealed that 97.2%, or 129.2 million internet users, in Indonesia have spent time on social media, and 63.5% or 84.6 million users, have done an online transaction. With a population of 256.5 million people in Indonesia, the internet users are still 132.7 million people, therefore, there is still possibility for ICT companies to find new consumers, especially for the internet market. The Indonesian government is encouraging the use of ICT in every aspect of business and urging society to participate in the implementation and development of technology. However, cloud providers should give legal certainty for cloud users related to the protection and security of the internet

---

[257]Ibid. (n 36).
[258] Indonesian Ministry Regulation 26/PER/M.KOMINFO/5/2007 regarding the Securing The Making Use of Internet Protocol Based Telecommunication Network, Article 1.
[259] Indonesian Ministry Regulation 29/PER/M.KOMINFO/12/2010 regarding Second Amendment to the Decree of the Minister of Communication and Information Technology Number 26/Per/M.Kominfo/5/2007 on Securing The Making Use of Internet Protocol Based Telecommunication Network, Article 1.
[260]'The 2016 Survey of Penetration and Behaviour of Indonesia's Internet User' (*Apjii.or.id*, 2017) <http://www.apjii.or.id/survei2016> accessed 3 February 2017.

services.

Kaufman[261] stated that providers of the cloud should make sure that they protect the confidentiality, integrity and availability of its consumer data, and make sure that their storage meets the minimum security requirements, including encryption, authorisation access and data backup. Kaufman stated that there is a need for the provider to make sure on the standard security system, however, the discussion later arose related to who will be responsible for the data security in the cloud.

Gonzales[262] stated that there are numbers of security concerns related to the implementation of cloud computing. He explained that network security (including transfer and configuration), interfaces (including authentication), data security (including cryptography and disposal), virtualisation (including data leakage), governance (including data control and security control), compliance, and legal issues (including e-discovery and provider privilege) have all affected the adoption of cloud computing. He suggested that there should be a security level that can provide for the security concerns of the cloud. If we refer to the statements of the policy makers in Indonesian ICT companies and through the regulation on ISMS, they provide adequate protection. However, more communication between units and departments is needed to support the implementation of the security system by all employees.

Jaatun[263] stated that specific protection related to the cloud security is needed to cope with current technology. Basu,[264] Jaatun,[265] Watson[266] and Cayirci[267] have proposed several alternative solutions to comply with the security protection in the cloud.

Blount and Zanella[268] take the view that infrastructure, applications and data,

---

[261]Ibid. (n 200), Lori M. Kaufman.
[262]Ibid. (n 200), Nelson Gonzalez et al.
[263]Martin Jaatun, Costas Lambrinoudakis and Chunming Rong, 'Special Issue on Security in Cloud Computing' (2012) 1 Journal of Cloud Computing: Advances, Systems and Applications.
[264]Anirban Basu et al., 'Privacy Preserving Collaborative Filtering for SaaS Enabling PaaS Clouds' (2012) 1 Journal of Cloud Computing: Advances, Systems and Applications.
[265]Martin Jaatun et al., 'The Design of a Redundant Array of Independent Net-Storages for Improved Confidentiality in Cloud Computing' (2012) 1 Journal of Cloud Computing: Advances, Systems and Applications.
[266]Paul Watson, 'A Multi-Level Security Model for Partitioning Workflows Over Federated Clouds' (2012) 1 Journal of Cloud Computing: Advances, Systems and Applications.
[267]Ibid. (n 200), Erdal Cayirci et al.
[268]Ibid. (n 188).

software, hardware, and servers all constitutecloud services, and this is in line with the spirit of the Indonesian regulations. Government Regulation 82/2012[269] and the Ministry Regulation 4/2016[270] state that an electronic system is: 'a series of devices and electronic procedures that serve to prepare, collect, process, analyse, store, display, publish, transmit, and/or distribute Electronic Information'. Therefore, the ICT providers that provide services related to an electronic system have the obligation to comply with the rules and regulations. They need to be clear that customers have complete protection on the internet, from preparing the system to distribution of the content. In addition, those circumstances have been guaranteed by law.

Ministry Regulation 4/2016,[271] through risk management, required that electronic system providers should provide security management system information for the public. The regulation also required that providers should refer to the SNI (Indonesian Standard version) ISO/IEC 27001 security standard, adopting its standardisation of classification, labelling, asset handling, protection of records, privacy and protection of personal data.[272] The spirit of the regulation is to achieve recognition from other countries on the protection of information. Indonesia's government is optimistic of achieving ISO/IEC 27001 certification, and that the protection of data in Indonesia will be equal with that of other countries.

The security standard in ISO/IEC 27001 is not merely control of IT infrastructure security, but also the human resource policies on how to manage information security. If we look at the terms of ISMS in ISO/IEC 27001, it states that:

> '…part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources'.[273]

ISO/IEC 27001 is identifying the risk within the company, from the process, infrastructure, and the human resource. It was issued in UK in 1999, and consist of

---

[269]Ibid. (n 253), Article 1.
[270]Ibid. (n 10), Article 1.
[271]Ibid. (n 10), Article 2.
[272]Ibid. (n 115).
[273]Ibid. (n 115).

two parts, first is the code of practise (known as BS 7799-1) and the second (known as BS 7799-2) is added next as the specification for ISMS that deploy controls form the BS 7799-1. It was revised in 2005 by introducing by a new term, which is ISO (International Standards Organisation) and the International Electrotechnical Commission (IEC), which was updated in 2013.[274]

In the UK, Data Protection Act 1984 was introduced with basic rules of registration data and right to access to that data. The parties signed in the Convention 108 was undertaken to have an equal protection in personal data with the Convention 108. The registration data and right to access to the data is important to overcome the use of computer which was raised in the 1970s. The Younger Committee on Privacy made a recommendation (Cmnd 5012, 1972) and it was then responded by the UK government through a White Paper (Cmnd 6353, 1975). The government stated that whoever used a computer should handle personal information responsibly. The UK government then set the Lindop Committee to set up a Data Protection Authority (Cmnd 7341) to be responsible for data privacy.

Data protection in UK law is based on the Convention for the Protection of Individuals regarding Processing of Personal Data (the Strasbourg Convention) from 1981. In the convention, the individuals' rights and freedoms are highly protected, as is privacy and personal data. This Convention becomes the basis of UK's Data Protection Act (DPA) 1984.[275] The UK's DPA 1984 was the law on processing the personal data that should be comply.[276] The adoption of EU Directive 95/46/EC[277] in October 1995 led to a new data protection framework with the DPA 1998.[278] This regulated the lawful protection of individual's privacy on the processing of personal data through its principles.

The UK Information Commissioner's Office (ICO) explains that DPA 1998 is highlighting eight personal data principles.[279] It stated that personal information must

---

[274]Ibid. (n 115).
[275]Data Protection Act 1984.
[276]Peter Carey and Peter Carey, *Data Protection* (Oxford University Press 2009)
[277]Ibid. (n 25).
[278] Data Protection Act 1998.
[279]'Guide to Data Protection' (*Ico.org.uk*, 2016) <https://ico.org.uk/for-organisations/guide-to-data-protection/> accessed 18 July 2016.

be processed for limited purposes, fairly and lawfully according to the data subjects' right. It should be accurate and up to date, adequate, relevant and not excessive. It must be kept in a secure place for a certain period with authorisation and it should not be transferred overseas without sufficient protection. Sufficient protection means that the third country should have an adequate protection through its national law or have ratified the international rights of data subjects.

This Act is proposed to organise on how organization react to the protection of personal data in the company. Company, big or small size company, hold some personal data, whether it is employees' personal data or customer's data. Therefore, it is important for all employees to be aware to its function in the company that he or she is dealing with such data, moreover when the data is use and store in their premises. Breaching of personal data can affect the business, therefore, all employees should be aware and understand the consequences of data breaching in the company.

In section 55 DPA 1998, there are explanation related to unlawful obtaining of personal data. It stated that:

> A person must not knowingly or recklessly, without the consent of the data controller—
> (a) obtain or disclose personal data or the information contained in personal data, or
> (b) procure the disclosure to another person of the information contained in personal data.

It is essential for company that deal with personal data, to make sure that they have protect the personal data of the data that being kept in the premises properly and make sure that they have done such protection in accordance to the principles in the DPA 1998. Whether as data processor or data controller, they must comply with the DPA 1998, to make sure that they have done a minimum standard of data protection in the premises, to enforce special rules on transborder data, and to support the national data protection authorities.[280]

Numbers of enforcement notice has been done by The Information Commissioner's Office (ICO), such as: has fined Vote Leave Limited £40,000 for sending out

[280]Adam Warren, 'Fully Compliant? A Study of Data Protection Policy In UK Public Organisations' (Ph D, Loughborough University 2003).

thousands of unwanted text messages related to the 2016 EU referendum without any consent,[281] case of Shamim Sadiq who worked at Hollybrook Medical Centre in Littleover, Derby that has been fined £120, plus £364 costs and a victim surcharge of £30, for sending personal data of her patients to her own email without authorisation,[282] case of Kevin Bunsell who accessed the authority's recruitment system and emailed the personal information, included the name, address, telephone number and CV to his partner's Hotmail account. He was fined £660, plus costs of £713.75 and surcharge of £66,[283] case of Darren Harrison, of Twickenham who obtain personal data included names, unique pupil numbers, along with performance management data for staff and uploaded the data onto his former school's servers. He was fined £700, plus costs of £364.08 and surcharge of £35.[284]

Another case is the case of *Arthur J. Gallagher Services (UK) Limited and others v Skriptchencko and others,*[285] The Court had to decide related to the deletion of confidential data of the previous company from the employee's computers and electronic devices. Another case of Mark Lloyd. He was the employee of Acorn Waste Management Ltd (Acorn) when he collected 957 of his client data into his own email, which contained his client's personal information and sensitive information and he about to leave Acorn to work for a competing company. Lloyd appeared at Telford Magistrates Court in 2016 and was prosecuted under section 55 of DPA 1998 for unlawfully obtaining personal data and he was fined for £300, pay a victim surcharge of £30 and £405.98 in cost.

Those cases have shown that it is important for all employees to understand the importance of personal data protection awareness in the workplace. From the cases above, most of the violation of the law is related to computer and its development technology in the workplace. Therefore, the protection related to data privacy is not

---

[281]'Vote Leave Limited' (*Ico.org.uk*, 2019) <https://ico.org.uk/action-weve-taken/enforcement/vote-leave-limited/> accessed 11 April 2019.
[282]'Shamim Sadiq' (*Ico.org.uk*, 2019) <https://ico.org.uk/action-weve-taken/enforcement/shamim-sadiq/> accessed 11 April 2019.
[283]'Kevin Bunsell' (*Ico.org.uk*, 2019) <https://ico.org.uk/action-weve-taken/enforcement/kevin-bunsell/> accessed 11 April 2019.
[284]'Darren Harrison' (*Ico.org.uk*, 2019) <https://ico.org.uk/action-weve-taken/enforcement/darren-harrison/> accessed 11 April 2019.
[285][2016] EWHC 603 (QB)

merely on data protection, but also on how providers can protect the technology system to support the delivery service. Technology required protection.[286] There will always be consequences from the implementation of technology,[287] and one of the concerns is the misuse of technology. In the UK, several cases in concerning the misuse of computers have given an insight into the lawful protection and prevention on the security and information system. In *R v Sunderland*,[288] a bank employee misused her authority to steal money from an account using the bank's computer. *DPP v Bignell*[289] revealed that it is prohibited to access an office computer for individual purposes. *Denco Ltd v Joinson*[290] showed that it unlawful to misuse an unauthorised password to access a computer, and in *Pickersgill v Employment Service,*[291] an employee illegally broke the access of another employee's computer. Those cases reflect that temptation of using authorised access in the workplace is high.

To prevent the misuse and data breach by an unauthorised person, the UK passed the Computer Misuse Act (CMA) 1990.[292] This tightens the law in crimes that involve computers. It states that to access any personal information on the computer system, each person should have their own authorisation. It also set the protection on the spread of malicious and damaging software. The CMA gives supporting protection on data that is stored on the computer premises and how people should treat the information. The importance of this Act is because manipulation from the development of technology has grown rapidly through computer equipment by employees.[293] Software piracy,[294] using companies' internet access for their own purposes,[295] and sharing passwords and sensitive information[296] are found in the

---

[286]M.G. Adamiaket al., 'Wide Area Protection—Technology and Infrastructures' (2006) 21 IEEE Transactions on Power Delivery.
[287]M. Igbaria and M. Tan, 'The Consequences of Information Technology Acceptance on Subsequent Individual Performance' (1997) 32 Information & Management.
[288] Unreported, 20 June 1983.
[289][1988] 1 Cr App R 1.
[290][1991] IRLR 63.
[291] [2002] EWCA Civ 23.
[292]Computer Misuse Act 1990.
[293]John D'Arcy and Sarv Devaraj, 'Employee Misuse of Information Technology Resources: Testing A Contemporary Deterrence Model' (2012) 43 Decision Sciences.
[294]A. Graham Peace, Dennis F. Galletta and James Y. L. Thong, 'Software Piracy in the Workplace: A Model and Empirical Test' (2003) 20 Journal of Management Information Systems.
[295]Vivien K. G. Lim, 'The IT Way of Loafing on The Job: Cyberloafing, Neutralising and Organisational Justice' (2002) 23 Journal of Organisational Behaviour.

misuse of technology in the office.

First introduced in 1990, Computer Misuse Act was intent to prohibit anyone of accessing unauthorised access to computer. It was triggered by the case of *R v Gold &Schifreen*[297] which in 1984-1985 break the authorization access of BT's Prestel and gained the access to Prince Phillip among others. They were charged under Forgery and Counterfeiting Act (1981) for defrauding BT using a "false instrument" and fined £750 and £600 respectively. Computer Misuse Act 1990 was made to keep the access to computer material, access to commit offences, and from modification of computer material. There was no exact definition of computer due to the rapid development in technology, however, in *DPP v McKeown*, *DPP v Jones*, Lord Hoffman defined computer as "*a device for storing, processing and retrieving information.*"[298]

In CMA 1990, the liability for offences should be either the accused or the target computer being in England and Wales, however, if the offender posted material by server in United States, they could be tried in UK, as in the case of *R v Smith (Wallace Duncan)*[299] and *R v Sheppard*.[300]

The Computer Misuse Act has a few amendments with the most significant amendment made in 2015. The amendments are mostly due to the development of technology and a result of the changes made by sections 41 – 44 of the Serious Crime Act 2015, as we can see in the case of *R v Mudd*,[301]*R v Crosskey (Gareth)*,[302]*R v Mangham (Glen Steven)*.[303] Therefore, it is necessary to have regulation or policy to maintain the ethics of employees or people who are authorised to manage data and information in the workplace.

2.2.3 The data controller and data processor

Cloud computing is a business model with benefits that simplify and reduce the

---

[296]MonideepaTarafdar, Ashish Gupta and OfirTurel, 'The Dark Side of Information Technology Use' (2013) 23 Information Systems Journal.
[297](1988) 1 AC 1063
[298] [1997] 2 Cr.App. R. 155, HL
[299] (No. 4) [2004] EWCA Crim 631 Q.B 1418
[300] [2001] EWCA Crim 65
[301] [2018] 1 Cr App R (S) 33 (7)
[302] [2012] EWCA Crim 1645; [2013] 1 Cr.App.R.(S) 76
[303] [2012] EWCA Crim 973; [2013] 1 Cr.App.R.(S) 11

expenses of a company on technology. Leimeister[304] stated that cloud users could outsource their technology requirement to the cloud provider; not only the technology, but also the service and maintenance of the cloud. This makes cloud computing significant technology in the business.

Teneyuca[305] stated that only few cloud computing training and security concerns have slowed down the implementation of the cloud. Lack of control and supervision in cloud computing are also a consideration for users.[306] It is important for the cloud provider to have control of their employees to protect the consumer. This research will elaborate on the role of data controller and data processor in the cloud company. It is important to have an in-depth function of data controller and data processor in the company, since they have to manage data security and data privacy for users. Companies who act as data controller or data processor should understand their responsibility to avoid any violation of the user's data.

The terms data controller and data processor can be found in DPA 1998, and is defined in EU Regulation 2016/679 as:

> '[the data controlled is] the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.[307]

> [the data processor is]'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.[308]

To protect user's personal data in cloud service, the cloud provider should be able to determine whether they act as a data controller or a data processor. Data Protection Act 1998 is important to protect data that is being help in the premises. As stated before, it has eight principles of protection. However, with the implementation of GDPR 2018, DPA 1998 was upgraded into DPA 2018 by providing how data

---

[304]Ibid. (n 157).
[305]Ibid. (n 61).
[306]Richard Chow et al., 'Controlling Data in the Cloud' [2009] Proceedings of the 2009 ACM workshop on Cloud computing security - CCSW '09.
[307]Ibid. (n 26), Article 4 (7).
[308]Ibid. (n 26), Article 4 (8).

protection law is being implemented in UK and set out separation of law enforcement authorities, national security and defence, and Information Commissioner's functions.[309] At the time when the thesis was made, DPA 1998 was still in force; however, it has now been repealed and replaced by the DPA 2018. Therefore, the reason for focusing on the DPA 1998 is because of the newness and consequent lack of cases in the respect of the DPA 2018.

The ICO[310] states that the data processor should do any activities associated with technical aspects, while the data controller carries any decision related to personal data. The separation clearly sets the responsibilities in protecting personal data. The idea of positioning the role of data controller and data processor is to determine the responsibility of each, and to make sure that each carries out their responsibility for protecting personal data.

EU Regulation 2016/679[311] has strengthened the importance of personal data protection. Through each section in the Regulation, the EU has regulated that organisations should protect personal data. It is important to have a certain organisational responsibilities to give adequate protection for the customer. The data controller could act as the front line in the company. They need to make sure that they have the responsibility for collecting the customer data, classifying data that contains personal data, how to use the data, who can access the data and how to maintain the data. The data processor acts like a technical section that must make sure that the IT infrastructure works properly. They also need to make sure that they store the personal data securely, and that they follow the procedures on the maintenance of personal data. It is important for companies and their employees to understand and comply with the Regulation. Compliance should also be followed by other countries that working together with EU in such cooperation. They should have the same perspective on the personal data protection. Looking at the Blue Book,[312]the EU has committed to

---

[309] 'About The DPA 2018' (*Ico.org.uk*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/> accessed 22 April 2019.
[310]'Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are' (*Information Commissioner's Office*, 2014) <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> accessed 19 July 2016.
[311]Ibid. (n 26), Article 5.
[312]Ibid. (n 98).

support the development of technology in Indonesia. Therefore, it is necessary for the Indonesian government to have the same perception on how to protect personal data.

The Regulations released in December 2016, regulated two significant segments on the personal data protection. These regulations have become an important part for the development of technology, especially the cloud.Ministry Regulation 20/2016, stated that processing, in terms of personal data starts, from the process of collection, organising, processing and analysing, storing, retrieving, publishing, disclosure, dissemination or making available, and erasure or destruction. Ministry Regulation 20/2016 states that electronic systems operators should have their own internal policy in processing the personal data protection, regarding the implementation of technology, human resources awareness and updating employees' skill, and methods and expenses. An electronic system operator is defined in Government Regulation 82/2012 and Ministry Regulation 20/2016 (see above).

Ministry Regulation 20/2016[313] then elaborates on the responsibility of the electronic system operator. Those are to perform the electronic system capability certification, to perform the personal data protection, and to inform the personal data owner through written notification whenever there is a failure on performing data protection managed by them. It is also to have internal policy on the personal data protection and to provide an audit record related to the personal data protection. The electronic system operator should make sure they have provided consent to the personal data owner related to the using of the data to the third party, to give an access to the personal data owner to adapt or alter their data, or to delete or dispose the personal data. They need also to provide a contact person in the relation of the personal data processing.

If we look in EU, GDPR has distinguished the role of data controller and data processor. The distinction is for the importance of compliance between data controller and data processor, stating their responsibility and role in the protection of personal data. Data controller determines purposes and means of processing of personal data, while data processor acts on behalf of data controller. Each organisation that deals with personal data must treat the data properly. The strict task and classification of

[313] Ibid. (n 11), Article 28.

each organisation would not cause an overlap in the organisation; furthermore, if there were an obstacle in the task, it would not take a long to resolve it because each organisation knows its restrictions.

In the GDPR, personal data only collected by data controller, which makes data controller responsible for determining legal authority in the relation of the data, including establishment of the contract. Meanwhile, data processor obligated by law to follow the directions of data controller. Data processor should also inform the controller if there is infringes of the GDPR. However, data processor should aware to the limitation of its role, because at any time data processor is involve in collecting data, their role become data controller in the eye of the law.

GDPR has also mandate data controller and data processor to comply with to the code of conduct that has been set by GDPR. Clear role separation of data controller and data processor in GDPR has strengthened the law enforcement of personal data protection in EU. GDPR has set stricter requirement for data processor, such as, the appointed processor should have been comply to GDPR in the written agreement,[314] data processor should not appoint a sub-processor without written consent from data controller,[315] in the contract, data processor should ensure that they have an appropriate obligation of confidentiality to all authorised person of data processor.[316] In GDPR, for the first time, the processor is liable for the damage caused by processing when it has not complied with GDPR obligations or the controller's instruction.[317]

The GDPR also discuss the position of joint controller, which it has not been discuss yet in the Directive. It is stated that joint controller is when two or more controllers joint to determine the processing of personal data.[318] In GDPR, joint controller obligations is more clearly enforced, for example IaaS providers which only provide users with a managed hosting service must now take responsibility for processing data (such as logs) generated by their infrastructure. It should assign data protection

[314]Ibid. (n 26), Art.28(1)-(3)
[315]Ibid. (n 26), Art. 28(2), (4)
[316]Ibid. (n 26), Art 28(3)(b), 29
[317]Ibid. (n 26), Art 29
[318]Ibid. (n 26), Art. 26

compliance responsibilities in the relation of who's responsible of what. In the relation of supporting the business and partnership of EU and Indonesia as well as European Economic Area (EEA) and Indonesia, therefore, Indonesia should also need to strengthen their regulation in personal data protection. It is important for the ICT companies in Indonesia to be aware and understand their role in protecting the personal data in their premises.

If we look again to Indonesia law, Indonesia regulation has already managed the role of each party in the relation of data controller and data processor.

Government Regulation 82/2012 also has a similar term on data controller and data processor, however, it did not explicitly state that there should be two different organisations to handle the personal data. The fact that the electronic system operator could transfer their obligation to an electronic agent would make more bureaucracy whenever there is a matter related to the protection of personal data. It should state clearly on the contract between the personal data owner and the electronic system operator if the management of personal data would hand the electronic transaction that involves personal data to the electronic agent. Transferring the obligation to the electronic agent does not mean that the electronic system operator has also transferred their responsibility for protecting the personal data. They also need to make sure that the electronic agent complies with the regulations and policy related to personal data protection. However, Indonesian Law 11/2008 regarding Electronic Information and Transactions[319] states that if the electronic transaction is conducted through an electronic agent, all the transactions would become the responsibility of the agent. Electronic transactions include personal data verification. This responsibility transfer would eliminate the obligation for the electronic system operator to protect the personal data. The statement of electronic transaction on Article 21 of Indonesian Law 11/2008 will weaken the spirit of protecting personal data, since there is no certainty that the electronic system operator will protect the personal data or deliver the obligation to the electronic agent. However, since Ministry Regulation 20/2016 did not state that an electronic system operator could transfer the obligation to an electronic agent, it would assume that the organisation would manage their

[319]Indonesian Law 11/2008 regarding Electronic Information and Transactions, Article 21(2c).

responsibility themselves. This would require the organisation to have a policy on how the personal data should be managed. ISO/IEC 27001 is guidance on the protection of personal data through the information security management system in ICT companies. Nevertheless, organisations should also make sure that their employees have the same perception of the importance of personal data protection. Comprehension of the substantial protection in the new business model in the ICT business is important.[320] Employees should treat personal data carefully.

2.3 ICT Companies' Understanding in Responding to the implementation of Legal Issues in Cloud Computing

To deploy cloud computing as a business model, the cloud provider needs to prepare sufficient tools like software, hardware, platform and infrastructure, and prepare the employees to deal with the cloud service. By doing so, the provider could deliver a comprehensive cloud service owning, operating, maintaining and pricing to cloud users.[321] Companies should emphasise to all employees the importance of keeping up with the latest technology: not merely the technological aspects, but also the implementation of the technology. Understanding vulnerabilities such as data security or personal data will help shift the organisation to cloud computing.[322] Cloud providers need to improve so they can meet market demand. They need to have adequate performance and the best service to their clients or users. In the market, if a provider could not meet the expectation of the user, competitors will overtake it.[323]

This research will examine the implementation of cloud computing in Indonesia; therefore, it is necessary to look at future ICT developments there. The rapid development of IT in industry has forced the cloud providers to shift their traditional resource management into a modern architecture to meet the market demand. McKinsey & Company[324] released a report revealing that ICT readiness could bring

---

[320] Evin M. Tas, 'ICT Education for Development — A Case Study' (2011) 3 Procedia Computer Science.
[321] Sean Marston et al., 'Cloud Computing — The Business Perspective' (2011) 51 Decision Support Systems.
[322] Keiko Hashizume et al., 'An Analysis of Security Issues for Cloud Computing' (2013) 4 Journal of Internet Services and Applications.
[323] Ibid. (n 128).
[324] McKinsey&Company, 'Ten Ideas to Maximise the Socioeconomic Impact of ICT In Indonesia'

have a positive effect on economic growth. Industry analysts, Merrill Lynch and Morgan Stanley[325] have made a prediction that cloud computing is going to lead technology trends. Research by the International Data Corporation (IDC)[326] reported that cloud and IT outsourcing were rising areas in Indonesia's ICT market in 2016. The ITU[327] reported that Indonesia is in the 19th in the ICT development index rank and 115th in global rank. Cloud computing became an interesting business model in Indonesia mostly because it offered the benefit of deploying and outsourcing IT network that led to budget savings.[328] The Indonesia Ministry of Communication and Information Technology mapped the ICT issues in Indonesia,[329] which include low information literacy and cyber crime. ADB papers on Indonesia[330] stated that development of ICT has significantly increased with the government's plan for broadband, however support is still needed. One of the supports is by reforming the policy and regulation on cyber security. Those reports have shown that the development of ICT in Indonesia is still continuously growing, especially related to cloud computing, however, those reports have also stated that Indonesia is still in danger of cyber-attack related to data security and the readiness to accept the technology.

Mangula, van de Weerd and Brinkkemper[331] state that lack of knowledge of the cloud business model has become one of the obstacles in the implementation of cloud business in Indonesia's companies. Soliman[332] stated that the successful implementation of cloud computing leads to the transformation of organisation,

---

(2015).
[325] Rajkumar Buyya et al., 'Cloud Computing and Emerging IT Platforms: Vision, Hype, And Reality for Delivering Computing as the 5thUtility' (2009) 25 Future Generation Computer Systems.
[326]'Executive Summary, Indonesia ICT Market Landscape Study' (*International Data Corporation*) <http://mdecstaging.s3.amazonaws.com/2016/11/29/15/35/11/63cf68f4-f915-4831-99b9-f541a387300a/INDO-MDEC-Executive-Summary-vF3.pdf> accessed 21 February 2017.
[327]'Measuring the Information Society Report 2016' (*International Telecommunication Union*) <http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf> accessed 21 February 2017.
[328]Ibid. (n 73).
[329]'ICT Research and Development in Indonesia' (*Ministry of Communication and Information Technology Republic of Indonesia*, 2015) <https://www.nict.go.jp/en/asean_ivo/4otfsk00001ver81-att/a1436766621134.pdf> accessed 22 February 2016.
[330]Asian Development Bank, 'Promoting Information and Communications Technology in Indonesia' (ADB Indonesia Resident Mission 2015).
[331]Ibid. (n 73).
[332]Fawzy Soliman, 'Modeling The Appraisal of Cloud Systems' Implementation' (2012) 8 Journal of Modern Accounting and Auditing.

including IT and employees. The ICT company's employees' participation in the implementation of cloud computing is important for the development of cloud computing and the business as well. McKinsey&Company[333] stated that Indonesia need to increase the supply of skilled ICT workers to overcome the shortage of nine million skilled and semiskilled posts.

It is necessary for ICT companies to prepare their employees to encounter the development of technology. It is important for ICT employees to be aware to the impact of the implementation of new technology in the workplace,[334] especially in the relation of cloud computing.[335] As in the cloud system, data of employees, companies, and customers' will be kept in the companies' premises, ICT employees need to realise that they carried a huge responsibility to maintain and keep the data safely.[336] Humphreys[337] stated that human error is the biggest risk to the information system, and the UK cases on the misuse of computer in Section 2.2.2 involve employees. Most of the crime that involves computers is related to data protection breaches.[338] Employees have the authority to access any information related to their work, however, related to personal data, it should be a restricted.

Most employees should be aware of the restrictions related to company information access. It is important for high-level management to show a good leadership in terms of direction, authority, policy, governance, and organisation.[339] High-level management deal with policy formulation and goal setting of the company.[340] They have to make sure that they are informing their colleagues and employees about information security, and are placing the right people in the right job with the sufficient skills and experiences. Humphreys stated that: 'the organisation need to ensure that staff are aware of information security risks and have sufficient

---

[333]Ibid. (n 324).
[334] Mike Simmonds, 'Instilling A Culture of Data Security Throughout the Organisation' (2018) 2018 Network Security.
[335]Ibid. (n 212), Duha Alsmadi and Victor Prybutok.
[336] Kamal Halili Hassan, 'Personal Data Protection in Employment: New Legal Challenges for Malaysia' (2012) 28 Computer Law & Security Review.
[337]Ibid. (n 41).
[338] Ian Lloyd, 'From Ugly Duckling to Swan. The Rise of Data Protection and Its Limits' (2018) 34 Computer Law & Security Review.
[339]Ibid. (n 41).
[340]Robert N Anthony, *Planning and Control Systems* (1st edn, Division of Research, Graduate School of Business Administration, Harvard University 1981).

understanding to support the organisation's information security policy to undertake their normal work functions and tasks. Staff should be trained in the use of information security policies and procedures, security controls applicable to their job function and the correct use of IT (e.g., log in procedures, keeping passwords safe, appropriate use of IT)'.[341]

Annex A7 to ISO/IEC 27001[342] states that the human resource security factors are included in the cycle of prior employment, during employment, and termination and change of employment. Knowledge about information security risks could be deliveredthrough an education and training process. A company could perform training on information security risks through the induction for new staff, on-the-job-training, or annually.[343] The training content should cover information security and business risk, rules and guidelines, roles and responsibilities and commercial and legal aspects.[344] High-level management have to make sure that their colleagues are aware to the security system in the company.

ISO/IEC 27001 controls best practice in the IT companies, especially in information security. To ensure that the workforce remains qualified for roles within the company there needs to be an audit of skills against company needs, with access to a training cycle. It means that, companies have to make sure that they have some short and long-term plans for the employees in the companies. ISO/IEC 27001 stated that employee's control should start from the recruitment cycle until employee's termination. Company should be able not only the strategy of the company in the short and long term, but also to identify the skill sets needed to achieve the plan, which in turn enables an employer to identify training gaps/needs in the workforce, of which the employer should try to fill. This plan is state on the Corporate Strategic Scenario (CSS), which consist of company's short and long terms plan. CSS not only planning the business, but also planning on the human resource. On the plan, policy makers from within the company, should determine the next strategic plan for the development of the company's business.

---

[341]Ibid. (n 41).
[342]Ibid. (n 115).
[343]Ibid. (n 115).
[344]Ibid. (n 41).

To succeed in the strategies that they make, policy makers should also make an Annual Business and Budget Plan to see the opportunity for potential business.[345] A business plan can be described as a business goals, how to achieve it, and the plan to achieve it.[346] The Annual Business and Budget Plan is made to see the match between the necessities programme of each division in the company with the budget provided by the company in one year. The Annual Business and Budget Plan will provide a yearly programme of each division in the company. The approved programme will be put on the Annual Business and Budget Plan and it will be ratified by the Board of Directors and Board of the Commissioners. This plan is also known as an internal business plan.[347]It is a result of management agreement on strategy, budget allocation, job path, and also obstacles in the workplace to support the company's strategic business. It is to make sure that management has consistency in planning to support the business. An internal business plan might be a tool to evaluate whether the business aspects are working and to examine the benefit of the aspects in the company strategic business.

Benefits and compensation might be a trigger for employees to support the company in enhancing performance.[348] This includes training as a benefit for employees.[349] Training could support the company to identify the skills needed to achieve the company's strategy, to make sure that employees remain qualified for their roles in the workplace and to support the life-cycle of employment from recruitment, employment, until the termination of the employee.[350] Training can effectively support the productivity of employees and support the performance of the companies. It can also minimise the risk of data breach in the company.[351] If we look at Ministry

---

[345]Melodi Botha and Claire Leanne Robertson, 'Potential Entrepreneurs' Assessment of Opportunities through the Rendering of a Business Plan' (2014) 17 South African Journal of Economic and Management Sciences.
[346]Michael Anderson and Jane Khedair, *Successful Business Plans* (Crimson 2009).
[347]Ibid.
[348]Shawn M. Carraher, 'Turnover Prediction Using Attitudes towards Benefits, Pay, and Pay Satisfaction among Employees and Entrepreneurs in Estonia, Latvia, and Lithuania' (2011) 6 Baltic Journal of Management.
[349]Herman Aguinis and Kurt Kraiger, 'Benefits of Training and Development for Individuals and Teams, Organisations, and Society' (2009) 60 Annual Review of Psychology.
[350]Ibid. (n 41).
[351] Michael Fimin, 'Five Steps to Protect Confidential Data When Employees Leave' (2017) 2017 Computer Fraud & Security.

Regulation 8/2014, it is stated that training is a whole activity to support and develop the employees' competency at work, including productivity, work ethic, and level of skill and expertise in accordance to the level and qualification at the workplace. The Ministry Regulation has stated that it is necessary for companies to make sure that their employees have already been provided with knowledge for their own benefit, and to meet the qualification needed by the company. Further on, Ministry Regulation 8/2014 states that the objective of the training in the company is to make sure that employees meet the Indonesian working standard competence, special standard or international standard. Training is important in the company to find the employee who is not performing their task effectively because of deficiency of skill or knowledge, or who needs to learn new skills.[352]

To support those objectives, there should be appropriate forms of instruction, assessment, and certification in training.[353] Generally, there are two types of training, competence training and leadership training. Competence define as an individual attribute of personality, specific skill, measurable performance within a work role,[354] while leadership is designing to form an individual leadership skill to improve the performance of specific requirement in the company.[355]

To have sufficient training, organisation might have a validation and evaluation of its training cycle. Validation is done to test how effective the training to the work performance of the trained employees.[356] In conducting training, management should consider the training process, methods, tools, constraints of trainees and trainers and organisational factors.[357] An organisation often deploys a training process that involves defining the need, planning, delivery and evaluation.[358] Even though a study[359] has indicated that some elements of a Personal Development Review (PDR)

---

[352]Tony Newby, *Validating Your Training* (Kogan Page 1992).
[353]Curtis J Bonk, 'Online Training in An Online World' (2002) 16 USDLA Journal.
[354]Ibid. (n 352).
[355]Julia C. Phillips et al., 'Society of Counselling Psychology Leadership Academy: Cultivating Leadership Competence and Community' (2017) 45 The Counselling Psychologist.
[356]Tony Newby, *Validating Your Training* (Kogan Page 1992).
[357]Ajit Kumara, Saurabh Bhatiab and I-Jen Chianga, 'Deployment of an In-House Designed Training Process in a Quaternary Care Hospital' (2013) 21 Technology and Health Care: Official Journal of the European Society for Engineering and Medicine.
[358]Leslie Rae, *How to Measure Training Effectiveness* (3rd edn, Gower 1997).
[359]Claire Baldwin et al., 'Personal Development Review (PDR) Process and Engineering Staff

such as performance review, skill development plan review and reward review motivate staff, it is important to have such considerations that become the indication of Personal Development Review (PDR) of the training process. Beside those activities, it is important to have a good quality of the training content and delivery as a motivation for employees to learn,[360] encourage the improvement of skill-based learning[361] and to apply it in their workplace.[362]

The Indonesian Manpower Act[363] states that:

> 'Job training is the whole activities of providing workers or potential workers with, and paving the way for them to acquire, enhance and develop job competence, productivity, discipline, work attitude and ethics until a desired level of skills and expertise that match the grade and qualifications required for a position or a job is reached'.

According to this Act, employees should be provided with certain skill to develop their job performance. Ministry Regulation 8/2014[364] states that competency-based training in the company is held to master the knowledge, skills, and attitudes based on the standard. Both Act and Regulation in Indonesia have supported the employee to improve themselves and achieve the competence. This training should contribute to the company[365] depending on the position of the employees.

Each division in the company should make their plan related to the training needed in their division. To make the training plan, the views of the employee can be taken on board where training needs are identified in the PDR. The company should have an assessment of the employees' skill with the job requirement in the company periodically.[366] Therefore, to achieve the expected result of training, employees should be aware of the purposes of the training and participate in the training evaluation to

---

Motivation' (2014) 25 Journal of Manufacturing Technology Management.
[360]Janet H. Marler, Xiaoya Liang and James Hamilton Dulebohn, 'Training and Effective Employee Information Technology Use' (2006) 32 Journal of Management.
[361]Jason A. Colquitt, Jeffrey A. LePine and Raymond A. Noe, 'Toward an Integrative Theory of Training Motivation: A Meta-Analytic Path Analysis of 20 Years of Research'. (2000) 85 Journal of Applied Psychology.
[362]Ibid. (n 376).
[363]Ibid. (n 39), Article 1(9).
[364]Ibid. (n 113), Article 1 (7).
[365]Teresa Pitman, 'Training Success' (2014) 37 Business and Economics--Banking and Finance.
[366]Ibid. (n 376).

determine training effectiveness.[367] The company should also consider the readiness of the training policies, training structures and the capacity of the trainers to support the successful of the training in the company.[368] For example in ICT companies, it is important for the management to make sure that all of the employees are aware of and comply with the information security.[369] The key aspect of employment in ICT companies is to understand the security system being used. This is important because ICT companies are dealing with the data which falls within ISO/IEC 27001. It is important for all employees to understand such a system fully, as without it they will be unable to carry out the protection of data security and personal data and thus unable to do their job.Their understanding might include not revealing account passwords, prioritising the authorisation consent, protecting information and personal data of employees, and using electronic devices, according to their function.[370] This guidance is important, since there is still no regulation in Indonesia that protects the privacy and personal data of employees.

Customers have to know that placing their data in the cloud mean that the company is responsible for the security of the data. However, Indonesian internet users are not completely aware of the importance of personal data protection because they have lost control of how the company manages their data.[371] A study indicated that the use of IT, particularly cloud computing for Small Business Enterprise, is still relatively low.[372] A study indicated that the high 'power distance' and low reliability of infrastructure has put Indonesia behind in adopting SaaS.[373] This study also revealed that it is important to educate the industry and give a positive influence from the management with knowledge and favourable attitudes to support the development of

---

[367]Ibid. (n 15).
[368]Peter J. Smith, 'Learners and Their Workplaces: Towards A Strategic Model of Flexible Delivery of Training in the Workplace' (2001) 53 Journal of Vocational Education & Training.
[369]Inho Hwang and Oona Cha, 'Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance' (2018) 81 Computers in Human Behaviour.
[370]Ibid. (n 41).
[371]Antonio Alfredo Wijaya et al., 'Indonesian Awareness of Health Record Stored in Cloud Computing' [2014] 2014 International Conference on ICT for Smart Society (ICISS).
[372]K. Surendro and A. Fardani, 'Identification of SME Readiness to Implement Cloud Computing' [2012] 2012 International Conference on Cloud Computing and Social Networking (ICCCSN).
[373]Inge van de Weerd, Ivonne Sartika Mangula and Sjaak Brinkkemper, 'Adoption of Software as a Service in Indonesia: Examining the Influence of Organisational Factors' (2016) 53 Information & Management.

the cloud computing industry.[374] For that reason, security and the reliability of technology have become considerations for Indonesia's users to trust cloud computing.[375] With the number of internet users in Indonesia rising, cloud providers can still have a potential market. Therefore, it is necessary for policy makers to build awareness of security systems and data protection into their policy-making.

With the implementation of GDPR in May 2018, privacy officer were needed to make sure that the company has make a sufficient effort to protect personal data. Indonesia might learn from the experiences of the policy makers and executive authority of governments in the EU in protecting their personal data of its members.[376]

Policy makers should also make sure that policies related to the security system and personal data have been implemented properly in the workplace by all the employees. This is because all of the employees in ICT companies are dealing with the data security and personal data of themselves and the customers' data. Therefore, it is necessary for policy makers to keep the employees up to date with the policies and regulations related to data security and personal data protection. One of the ways that policy makers can do to make sure that those aspects are being implemented properly is by signing an integrity pact annually.[377] Usually, in an integrity pact, clauses control how ICT employees should comply with the policies related to the confidentiality of data. In the integrity pact, employees are challenged to comply with the fiduciary duties, good corporate governance, the duty of care principal, the responsibility principal, the duty of loyalty principal, and to comply with the conflict principal and the accountability principal. By signing this integrity pact, all ICT employees are aware and intentionally subject to company policies, and they also know the consequences if they break the policies.

---

[374] Sen Liu et al., 'Understanding the Effect of Cloud Computing on Organisational Agility: An Empirical Examination' (2018) 43 International Journal of Information Management.
[375]M Dachyar and Machadi Dhana Prasetya, 'Cloud Computing Implementation in Indonesia' (2012) 2 International Journal of Applied Science & Technology.
[376] Bart Custers and Bas Vergouw, 'Promising Policing Technologies: Experiences, Obstacles and Police Needs Regarding Law Enforcement Technologies' (2015) 31 Computer Law & Security Review.
[377]'Code of Ethics and Corporate Culture' (*Telkom.co.id*, 2018) <https://www.telkom.co.id/servlet/tk/mobile/about/en_US/stockdetail/code-of-ethics-and-corporate-culture.html> accessed 29 June 2018.

This integrity pact is also part of ISO/IEC 27001[378] clause that instructs ICT companies to make sure that they have establish, review and maintain a security system. The guidance in ISO/IEC 27001 and EU Directive 97/66/EC have highlighted the importance of data security and data protection skills in ICT companies, especially, and this awareness should also be realised in the policy-making in the companies. ICT companies cannot be detached from data security and data protection. Policy makers should provide sustainable training related to those aspects,[379] not only for employees who are in the technical tasks, but also for those not related to the technical task in the company, such as the billing division, legal division, or customer service division.

2.4 Chapter Summary

Cloud computing a combination of technologies that store information making cloud computing a new business model.[380] There are choices in the cloud delivery services and deployment model which are important for the user. Aside from the benefits offered by cloud computing, there are several considerations that cloud user should aware of which is relate to data security and personal data protection. Cases on the misuse of computers have revealed that it is necessary for cloud users to understand the impact of cloud computing in protecting personal data.

EU regulations and UK law place a strict protection on personal data and regulate the organisations that manage it. However, this strict control is not clear in Indonesian regulation. Despite the regulations promulgated in 2016, Indonesian regulation has not clearly stated the classification of personal data that should be protected by the provider. It also seems not to emphasise the important role of the controller and the processor on the process of protecting personal data. Indonesian regulation states that electronic system operators (which are data controllers in the EU) could shift their responsibility to an electronic agent if the electronic transaction is delivered by theagent. This could make electronic system operators deny responsibility for the

[378]Ibid. (n 115).
[379]Sureerut Inmor and Rungsun Suwannahong, 'The Acceptance of Cloud Computing for IT Workers in Thailand' (2017) 121 Procedia Computer Science.
[380]Ibid. (n 155).

protection of personal data. A strong restriction on the controller and processor of personal data would make the personal data owner feel confident with their personal data protection when they use cloud computing as a business model. The legal certainty on the responsibility of data controller and data processor will also make cloud provider assure their role and responsibility.

Legal certainty on the definition of data controller and data processor is important for cloud computing providers to make sure that their customers' personal data is protect appropriately. Regulations in the EU, UK and Indonesia have controlled the use of computer and electronic systems. The use of ISO/IEC 27001 as a guidance would guide how management needs to make sure that all employees comply with the security system. It is the obligation of the company to make sure that employees aware to the importance of the security system in the workplace and apply it to their job. However, to make sure that they have adequate skill and knowledge, management should offer training from the recruitment to the termination of the employees. This can be in the form of induction, on-the-job-training, or annual training. It is the company's policy to manage the training in the company.

Chapter 3. Methodology

3.1 Introduction

This chapter will describe the methodology used to answer the research questions. It will describe the detail of the approaches taken, and then discuss the aims of the research and the approach used to analyse the data. It will also address the ethical issues that arose in the research. This chapter then end with the constraints during the research process.

3.2 Aim of Research

Research is a way to develop a logic and rational way of thinking to solve a problem that includes technique and skill. Kumar[381] stated that research comes from two syllables, re and search. It means to seek a new or find a deeper aspect by examining it careful and methodically and then to test it to establish a new knowledge. According to Oxford Learner Dictionaries,[382] research is a specific study which aims to reveal novel facts. Gomm[383] explained that research is an activity of study to seek and clarify something that we believe. In the end, the result of the study is to reassure either that we are right or wrong. However, Dane[384] has a simple definition of research; research is a critical process to answer questions systematically and in doing the process will include a method to support it. All of these definitions mentioned that research raises a question and phenomena to be answered and requires methods to seek the cause or answer, and test the answer to the questions and theories to support the findings. To research is to understand problem and it involve a process to do it.[385]

3.2.1 Research methodology

There are several considerations if someone wants to start doing research. First, the

---

[381]Ranjit Kumar, *Research Methodology* (1st edn, Sage 2009).
[382]'Research_1 Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced Learner's Dictionary at Oxfordlearnersdictionaries.Com' (*Oxfordlearnersdictionaries.com*) <http://www.oxfordlearnersdictionaries.com/definition/english/research_1?q=research> accessed 4 October 2015.
[383]Roger Gomm, *Social Research Methodology* (1st edn, Palgrave Macmillan 2008).
[384]Francis C Dane, *Evaluating Research* (1st edn, Sage 2011).
[385]Beverly R Dixon et al.,*A Handbook of Social Science Research* (1st edn, Oxford University Press 1992).

researcher should ask themselves if the topic is significant to recent phenomena. The next question is whether the phenomena can be researched, what the coverage of the research should be, how to do the research, and what might arise from the findings of the research.[386]

Doing research is a process of knowing and seeking for an answer to the phenomena that include several phases, which is called research methodology. It will begin with the research question and then focus on a specific aspect of selecting research method. With the method, the researcher will start to collect data to answer the research questions. After data has been collected, the researcher will link the data with the research question to get the findings and solution of the research.[387]

Methodology is:

> 'the science of method, or orderly arrangement; specif., the branch of logic concerned with the application of the principles of reasoning to scientific and philosophical inquiry'.[388]

The methodology is also the readiness of reading in the research structures. It includes premises, theoretical consideration and phenomena that develop logic to answer the research question. Therefore, the researcher must be able to explain the reason for choosing the specific research approach.[389] Geoffrey[390] stated that methodology is a process of conducting research that involves planning, research study, conclusion and findings. From those explanations, it can be concluded that methodology is a tool in the research that helps the researcher. It is used to build more comprehensive and systematic research that includes theory and practical aspects to conclude the findings of the research. The researcher should be able to choose appropriate tools to get precise findings.

Methodology in research begins with deciding the research object and then planning

---

[386]Martyn Denscombe, The Good Research Guide for Small-Scale Social Research Projects (1st edn, Open Univ Press 2007).
[387]Ibid. (n 385).
[388]'Methodology Dictionary Definition | Methodology Defined' (*Yourdictionary.com*) <http://www.yourdictionary.com/methodology#websters> accessed 26 August 2015.
[389]J Jonker and B. J. W Pennink, *The Essence of Research Methodology* (1st edn, Springer 2010).
[390]Geoffrey Maruyama and Carey S Ryan, *Research Methods in Social Relations* (1st edn, John Wiley & Sons 2014).

the process and ending with doing the research itself.[391] When researcher decides to start research, he or she need to formulate what has become a problem and start a literature review. The next step is to decide how to conduct the research. They need to have a research design to describe, justify and explain how the research question will be answered. After deciding the research design, the next step is to construct the research methodology. This process will begin with selecting the research instrument to collect data and then selecting a sample. After the sample has been determined, the most crucial step is to collect the data. It is crucial because it may involve ethical issues. After collecting data, the researcher should process and display it by writing up are search report.[392] The cycle in the methodology includes various methods. The researcher should be able to determine which method is the best suited for the research.

3.2.2 Research method

Research method is a certain chronological procedure that can be used during research.[393] It has to be systematic in observing, classifying and interpreting the data collected.[394] There are three methods used to answer research questions: the quantitative approach, the qualitative approach and mixed methods.[395] Each has its strong point and weaknesses. In selecting research methods, the researcher should determine the best approach to their data collection.[396] This thesis is to examine the social phenomena that occurred in ICT companies in Indonesia, and so the researcher must determine the most suitable method for doing social research.

In social research, variety methods of data collection and analysis have been used. Booth[397] introduced one of the first major social surveys and published *Life and Labour of the People in London*. He used a survey technique and statistical method to seek the extent of poverty in working class London. Evan-Pritchard,[398] Radcliffe-

[391]Ibid. (n 381).
[392]Ibid. (n 381).
[393]Ibid. (n 389).
[394]Ibid. (n 381).
[395]Ibid. (n 381).
[396]Ibid. (n 386).
[397]Patrick McNeill and Steve Chapman, *Research Methods* (1st edn, Routledge 2005).
[398]Ibid.

Brown and Molinowski[399] found out that the best way to investigate the behaviour of people is by living among them for sometimes. This is known as anthropological technique.

In the 1960s in Britain there was a significant change in research methods with the development of the informal or unstructured interview. During the 1970s, fieldwork and participant observation were more popular than survey.[400] There were two important developments of social research in 1980s. The first was the rise of feminist research and the second was the structuration theory of Anthony Giddens.[401] He introduced the use of the multiple methods of research, which are both quantitative (to explore the influence of social structure) and qualitative (to see the response of the social structure). Geoffrey[402] points out that an authentic research method has to be bound with the research subject. He noted that the numbers of people to be studied had influence on the involvement of the researcher. He said that to get the best result, the researcher should use a mixture of methods to check the accuracy of data collection. However, the use of multiple methods might produce broad data that can be difficult to analyse.

This statement has influenced the researcher in this thesis to implement qualitative methods to seek the specific response in ICT companies in Indonesia. Using qualitative methods from the specific interviewees should reveal the relationship of the impact of the phenomena in the ICT industry to ICT companies. The outcome of using this method is expected to have a rich data and meaning full insight as a result. Rich data can be seen as the knowledge in the social phenomenon.[403] In qualitative method it consists of participants' motivations and intentions, which become the centre of social science research and can be used for management and indentify work.[404] In collecting a rich data as a result, it should be accurate, precise and accountable that is obtained from the interviewees. Therefore, when using interview

---

[399]Ibid. (n 397).
[400]Ibid. (n 397).
[401]Ibid. (n 390).
[402]Ibid. (n 390).
[403] Ulrike Schultze and Michel Avital, 'Designing Interviews To Generate Rich Data For Information Systems Research' (2011) 21 Information and Organization.
[404] Ibid.

as a research method, researcher is expected to gain numbers of value information from the interviewees. That is the reason the interviewees are selected policy makers in Indonesian ICT companies and the company in this thesis is the biggest state-owned company and has become the leader in its core business. The result of this thesis will provide recommendations related to the law and regulation in Indonesia, especially in data protection and data security in the Indonesian ICT industry.

A qualitative approach is more descriptive and narrative. It uses an unstructured and flexible methodology by using less data from interviews, observations and case studies to identify and describe the phenomenon. It will cover several issues from fewer respondents and cases. Qualitative methods are used to explore experiences and perception. Therefore, its value is authentic, and it emphasises the description of variables.[405] The weaknesses of this method are that it is subjective and cannot be inferred to the population. However, in this study, qualitative methods are the most appropriate to reveal to what extent ICT companies in Indonesia have implemented the phenomena in cloud computing, especially the implementation of data security and data protection through ICT companies' policy.

Choosing the most appropriate methods could help researcher to do the research properly. In selecting the methods, the researcher should consider the nature of the research itself, the skill of the researcher and how the methods will answer the research questions. The researcher should also think about the time for completion of the research and the resources of the participants.

3.2.3 Research methods in law

Methodology and methods are common terms that is used in legal research.[406] Adopting a meaning from the Oxford English Dictionary,[407] conducting legal research means that researcher does a systematic activity in seeking a specific thing or person in the law field, with the purpose of contributing knowledge through careful observation and study of a subject and the result is in a form of written book, article or

---

[405]Ibid. (n 381).
[406]Dawn Watkins and Mandy Burton, *Research Methods in Law* (1st edn, Routledge 2013).
[407]Home: Oxford English Dictionary - Research, N.1 (*Oed.com*, 2017) <http://www.oed.com/view/Entry/163432?rskey=RPJnyl&result=1&isAdvanced=false#eid> accessed 26 August 2015.

thesis. Doing legal research always starts from a theoretical basis that leads to the research question and how the research question will be answered.[408] It means that methodology and methods have an important meaning in legal research.

The legal phenomenon in this research is to what extent the law has given sufficient protection to the development of technology in Indonesia. This protection is specific to the data security and data protection in ICT companies. It is to examine whether current regulation has given protection to the data to the companies, employees and customers, whether the regulation is applicable to Indonesian ICT companies, are employees aware of the regulations on data security and data protection, and whether the regulation should be updated.

There are several types of legal research methodologies.[409] They are black letter or doctrinal analysis, jurisprudence perspective (which includes legal realism, critical legal studies, feminist legal theory, critical race theory, queer theory, and post modernist theory of law, law and economics), socio-legal research, empirical research methods, and comparative legal analysis. This thesis uses empirical legal research. The empirical research methods are used to see how the law works in the real life. For example, what is the effect of legal change, how the law touches the society or how the law is enforced?[410] The selection of empirical legal research in this study is to reveal how Indonesian regulations accommodate the development and implementation of aspects in technology in ICT companies. It is also to examine to what extent ICT companies address the preparedness of themselves and their employees for the aspects of the development of technology related to data security and data protection. This methodology is also used to determine whether the current regulation has already given sufficient protection for the ICT industry, including ICT companies and their employees, and also protection for the customer. It will also reveal the effect of regulation and policy related to the implementation of new technology in ICT companies.

In empirical legal research, there are three ways to analyse data, classical content

---

[408]Robert Cryer et al.,*Research Methodologies in EU and International Law* (1st edn, Hart Publishing 2011).
[409]Caroline Morris and Cian Murphy, *Getting a PhD in Law* (Hart Pub 2011).
[410]Monique Hennink, Inge Hutter and Ajay Bailey, *Qualitative Research Methods* (1st edn, Sage 2011).

analysis, discourse analysis and grounded theory method.[411] Classical content analysis is used when researcher examines documents such as newspapers, reports or interview transcripts to find a legal phenomenon. In this thesis, the researcher is using interview transcripts to reveal the real situation in ICT companies related to the implementation of cloud computing. It will also reveal to what extent ICT companies have implemented regulation and policy related to data security and data protection and expose the constraints and solutions in the implementation of new technology.

Conducting legal research might use quantitative or qualitative as research. However, to assess the social phenomena, using qualitative as an approach is better than quantitative. Descriptive methods are often used in the qualitative method to figure out the nature of the phenomena, such as legal system and effect of the policy, which only can be explained by using in-depth methods.

3.2.4 Research methods issues

The methodology is one of the important aspects of research; it determines how the researcher will perform the research and answer the research questions. Issues in choosing the research methods are mainly dealing with time, manpower, budget and the topic of the research. Access to the respondent can also become a problem. The researcher will usually spend six months collecting the data and then will need another long period to analyse it.[412] It is important for the researcher to understand and equip themselves with knowledge and training on the methodology. Another issue that might arise in the research is dealing with an ethical issue. Ethical issues often appear when the researcher is dealing with qualitative research methods. In qualitative methods, the researcher often seeks the perception, beliefs and experiences of the participants, which sometimes involving sensitive issues.[413] The researcher should protect any part of human participation in research. This protection includes the right of the participant to stop being part of the research at any time, the right to withdraw any data that have been supplied, the right to refuse to answer or respond any question on the research methods, right to ask related to the procedure of the research methods

---

[411]Peter Cane and Herbert M Kritzer, *The Oxford Handbook of Empirical Legal Research* (1st edn, Oxford University Press 2010).
[412]Ibid. (n 397).
[413]Ibid. (n 410).

and right to be anonymised.

According to the Economic and Social Research Council, law doctoral research should consider six principles in ethical research. They consist of emphasising that research should consider integrity and quality. Both staff and subject should be well informed about the research and how to conduct the research and information confidentiality, including the subject of the research, free-will participants, avoiding harm to research participants, independence and freedom from conflict of interest.[414] The Belmont Report[415] identifies three basic principles in conducting research, which are respect for the participants, benefice and justice for the participants. These principles are similar to those of the Economic and Social Research Council. The report mentions adequate information about the research, free-will participation, no risk of harm to the participants, protection of identity and confidentiality.

Another issue on the research is related to the data protection. The Data Protection Act 1998 requires that the researcher should consider the data that been gathered during and after the research. There are eight principles of the Act, which guide researcher in treating the data. Personal data should be processed fairly and lawfully. It only can be used for specific purpose, should be relevant, accurate, and kept for specific time. It should be processed properly, should be kept properly, and lastly, personal data should not be transferred other than to a European Economic Area country unless the country has an adequate level of protection.[416]

The researcher should be able to assure the ethics committee that all of the procedures related to ethics and data protection are obeyed. This procedure is not only protecting the participants, but also protecting the researcher from the harm that can arise from the research findings.

3.3 Methods of Research

This section will highlight the methods that will be use in the research. It will discuss

---

[414]Ibid. (n 409).
[415]Ibid. (n 410).
[416]Geeta Aiyer, 'Global Investment Community Can't Afford to Ignore Sustainability' (*the Guardian*, 2014) <http://www.theguardian.com/sustainable-business/2014/nov/14/global-finance-community-principles-responsible-investment> accessed 18 November 2014.

the methodology approach and potential issues that might arise as a result of the research, as follows:

3.3.1 Aims

The research will analyse the ICT regulations related to data security and data protection in the implementation of cloud computing in the workplace in Indonesia. Accordingly, it will analyse the relevant of Indonesian, EU and UK policy and regulations. It will firstly conclude whether there is sufficient Indonesian policy and regulation to cope with the implementation of cloud computing in the ICT industry. Secondly, the relationship between the employee's skill in the ICT industry and the implementation of Indonesian cloud computing industry will be examined. There are two overarching aims of the research, as follows:

1. To analyse the extent to which the Indonesian cloud computing industry would be affected by wide-ranging data protection and data security law reforms.
2. To evaluate the potential impact that data protection and data security law reform could have on the position of employees in the Indonesian cloud computing industry.

This thesis is original and unique because the researcher is researching the phenomena occurring in her own workplace.

3.3.2 Methodology approach

There are multiplicities of approaches to the research methods in the law field. However, they can be divided into two categories. First is a methodology that focused on the law as a major entity, and second is a methodology that includes another discipline for investigating and concluding a legal problem.[417] Deciding a proper methodology in the research is much depending on the nature of the research project. Deakin[418] stated that the changing of the perspective of employment law has prompted researchers to seek for more methods in addressing the issues. He also mentioned that Kahn-Freund has said that empirical research has been studied to support the legal framework in industrial relations. Deakin said that the perception of workplace relations had made a significant change to support more comprehensive data in

[417]Ibid. (n 409).
[418]Ibid. (n 411).

practice. An empirical study of employment law has guided the researcher to establish more focus on variables. It can be used to analyse the coherence in the field of legal regulation and business in terms of employee protection. Empirical research is close to a socio-legal approach to law. It includes how the phenomena happen, what are the implications from the phenomena, what are the legal impact, how people are affected, and the experiences of the phenomena.[419]

Given the aim of the research, it will use empirical legal research as a method. This research is also to study law, legal process and legal phenomena and will use data. Interview has become the best approach to take in this study because it will reveal up-to-date data from the interviewees and depict the real situation which the interviewees work with every day.

Burton[420] explained that the first thing to start the research is formulating the research question. Then, continued with literature review and then to develop grounded theory. This is the process of collecting data at the same time as producing a theory and data analysis. However, in this research, the researcher will use classical content analysis, which will examine the interview transcripts.[421]

In data collection, the researcher used interview as a method. The interviewees were selected from the ICT companies which had the highest number of employees and companies that dealt with technology in Indonesia. This data collection will give an insight into the legal theory and the legal phenomena that occur in the company.

This research used descriptive analysis by using of Indonesia, EU and UK policy and regulation related to data security and data protection, and employment law. This is to see on how the legal problem is being solved in such country by looking through their regulation and policy. It is also to elaborate to what extent the EU and UK solved the problem related to the development of technology and its implementation and also the protection of the employees in the ICT companies.

---

[419]Ibid. (n 409).
[420]Ibid. (n 388).
[421]Ibid. (n 411).

3.3.2.1. Data collection cycle

This qualitative research method formulates research questions, reviews literature, integrates theory, develops a conceptual framework and finally selects fieldwork. The qualitative method is used to test inferences that arise from the research questions.[422] This research also used the deductive conceptual cycle to develop laws to collect data. The concept of the deductive approach is to analyse whether the hypothesis based on the certain observation of the phenomena is leading to confirmation or rejection.[423] Deductive reasoning uses the existing literature to develop a framework that might concept the data collection.[424]

This study design is suitable for this research because it will examine and analyse the relevant Indonesian and EU, and UK regulation and policy in data security and data protection, related to the growth of the Indonesian cloud computing industry. The selection of EU and UK law and regulations is because the EU and UK had already implemented data protection and data security regulations through Directive 95/46/EC. Since Indonesian had only just implemented the regulation in data protection and data security in 2016, the implementation and the effect of the implementation of such regulations could be an example for the Indonesian government.

A deductive approach analysed whether the Indonesian cloud computing industry was affected by wide-ranging data protection and data security law reforms. It is also answered whether the data protection and data security law reform could have an impact on the position of employees in the Indonesian cloud computing industry.

The hypothesis was formulated based on theory and literature in data security and data protection and employment law and was tested empirically. Data from the data collection was used to verify the research hypothesis.

There are three main ways of collecting data in qualitative research, direct observation, in-depth interviews and analysis of documents.[425] In this research,

---

[422]Ibid. (n 411).
[423]Roel Snieder and Ken Larner, *The Art of Being A Scientist* (1st edn, Cambridge University 2010).
[424]Ibid. (n 410).
[425]Ibid. (n 411).

researcher used in-depth interviews of those responsible for the implementation of technology and employee protection in the Indonesian ICT industry. It used a semi-structured interview with open questions that were prepared and consulted on with a supervisor. By using semi-structured interview, the researcher might have several guiding questions related to the research in a particular order. However, the questions might develop based to the interviewee's reaction and the discussions during the interview.[426] Having open questions in the interview might encourage interviewees to answer and elicit the question deeply. It might develop more information from the insight and opinion from the interviewee.[427] The purpose of using in-depth interview is because researcher would like to seek deep information and individual experiences from interviewees.

The information that the researcher collected using in-depth interview was related to the personal experiences of those responsible for the implementation of new technology such as cloud computing and employee protection in the Indonesian ICT industry. The method is used to seek their perspective on cloud computing, how legal implications of the new technology influenced the policy-making, how decisions were made, and their perception and motivation in the making of the decision or policy.

The research instrument was a semi-structured interview with an open question from literature and the opinion of the supervisor in the relation of data protection and data security, as well as employment law. It consists of an introduction, opening question, key questions and closing questions.[428] However, questions might have developed during the interview depending to the interviewee's responds. It was pilot-tested to give a better understanding of the questions. Durkheim stated:

> 'When, then, the explanation of a social phenomenon is undertaken, we must seek separately the efficient cause which produces it, and the function it fulfils'.[429]

The interviewees were selected from all the relevant personnel at the decision-making

---

[426]D Cohen and B Crabtree, 'RWJF - Qualitative Research Guidelines Project | Semi-Structured Interviews | Semi-Structured Interviews' (*Qualres.org*, 2006) <http://qualres.org/HomeSemi-3629.html> accessed 13 March 2015.
[427]Ibid. (n 410).
[428]Ibid. (n 410).
[429]Émile Durkheim, *The Rules of Sociological Method* (8th edn, Free Press 1964).

level because the researcher wanted to seek specific and detailed insight into the issues. It selected policy makers as the people in charge in making a policy, instead of interviewing directors of the companies. However, the policy makers interviewed who were selected and delegated by directors have the responsibility in the policy-making in the company. That policy makers positions were one level below the directors.

Following the pilot, some changes were made, especially related to questions which were unclear, or which caused miss-interpretation.

The eleven senior managers who were interviewed were the people who had the authority to make company policy that was later signed off by the directors. The participants were approached by email with a participant information sheet. The interviews were conducted in Indonesian, and recorded. Notes were also taken to supplement the information obtained. Since the interviews were in Indonesian, they were transcribed and translated by the researcher, and the final data checked by a proof-reader in the UK after the interview was conducted.

Under the Data Protection Act (1998),[430] there are several principles that the researcher should note. Those principles protect the interviewee and the researcher and are related to the ethical code. In doing research, the researcher should know who might access the data. In this research, supervisors might have the access to the data. The identity of the interviewees was protected, and their comments anonymised using alphanumeric codes (SM or M and A1-4 to C1-4). The anonymisation of the data was randomised so that it would not be possible to deduce who made which statements based on the order of the interviews. Data from the interview was only used for the purpose of the relevant research, was up-to-date. Recordings of interviews were deleted as soon as they had been transcribed and the recordings and transcriptions transferred via an encrypted USB stick. During and after the study, all data, including hard copies of transcripts or notes of the interview, were stored securely in a locked filling cabinet on University premises. Electronic data files were encrypted and stored on password protected University computers. All data was accessible only to the researcher. All data relating to the study will be securely destroyed ten years after the

[430]Ibid. (n 278), Section 33.

study has been completed.[431] The interviews took place on the company's premises. The researcher interviewed the participant after office hours or during lunch time, with the approval of the participants. The company will not have access to the original data, only the final data of the research. The research did not touch the commercially sensitive areas of the company; it only explored the participants' experiences in deciding the policy in the company.

This thesis is unique because the researcher gained access to the ICT companies in this thesis since she was working in one of the companies and the company itself has given its support to conduct the research. The researcher had unprecedented accesses to policy makers during the implementation period of the new company regulations developed to address technological changes and shifts in employment. However, the research, publication, thesis, and any other research reports, will not identify the respondents' names or positions and no statements will be attributed to named or otherwise identifiable persons. Respondents' positions in the company will only be referred to with the participant's permission, so long it is significant for the analysis presented, and the individuals concerned cannot be identified.

Three companies were selected for the research: PT Telkom, PT Telkomsel and Telkomsigma. Those companies are appropriate for this research because they have large numbers of employees and are providers of cloud computing in Indonesia. There were eleven interviewees, the policy makers in the division of the company which deals with policy in cloud computing and employment. The participants of the interview were selected from all relevant personnel at the decision-making level. They were all in the position of the strategic managerial and were decision makers in their company. The reason for choosing policy makers is because the researcher would like to seek the background, motivation and experiences of those who have the power and responsibility in deciding the company's policy. The researcher would like to have detailed insight from senior managers to reveal how the policy was made, implemented and the consequences that arose from the policy for the employees.

---

[431]Christine Milligan, Hazel Biggs and Libby Bishop, 'Meeting the Requirements of the Data Protection Act (1998)' (*Faculty of Health and Medicine (Division of Health Research), Lancaster University*) <https://www.lancaster.ac.uk/researchethics/1-7-dataproact.html> accessed 13 March 2015.

PT Telkom represents the ICT industry in Indonesia, because it has a significant numbers of employees with a huge proportion of the mature and unskilled employees at the top position.[432] It is a state-owned company and the biggest telecommunications company in Indonesia[433] and should support the government programme to develop employees' capability and support the welfare of the citizens of Indonesia. Both PT Telkom and PT Telkomsel have implemented cloud computing for their business models, and the cloud computing system has been provided by Telkomsigma, which is a subsidiary of PT Telkom.

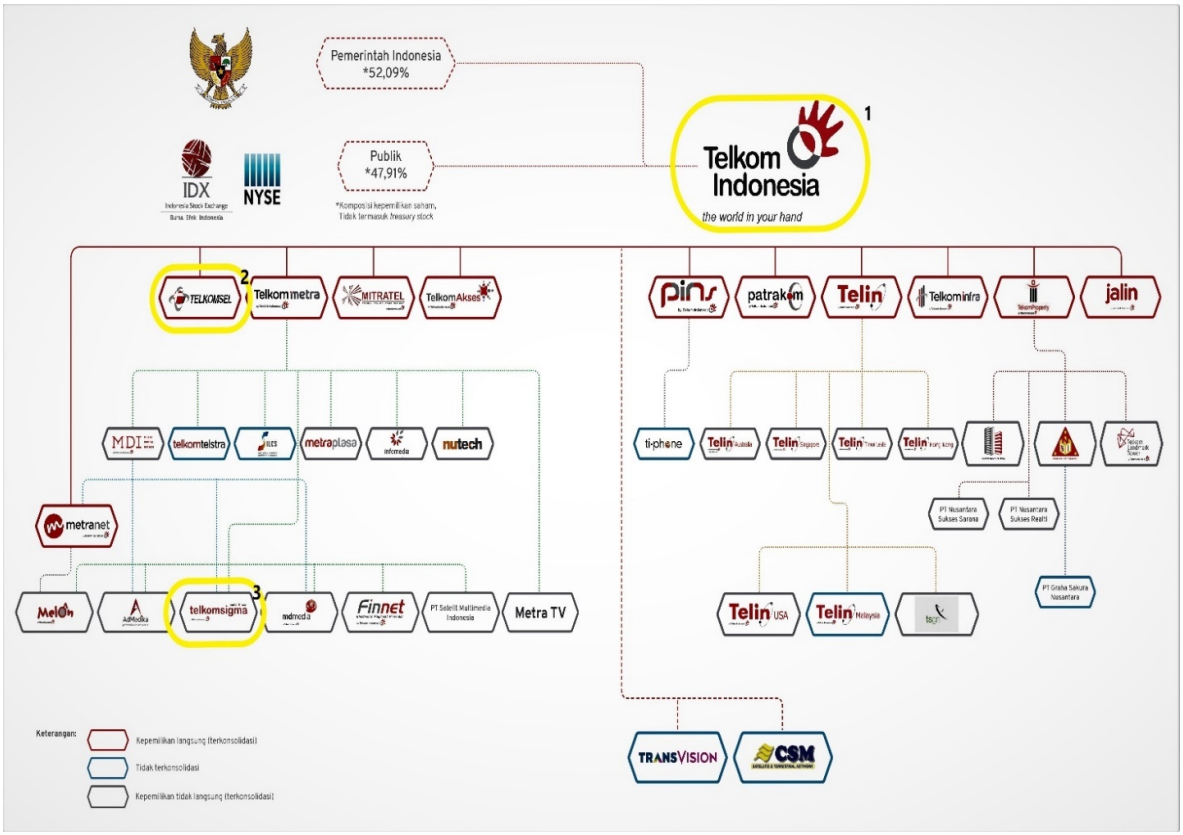

Figure 1.Company Structures

Telkomsigmais the leader in data centre and cloud computing in Indonesia.[434] With those characteristics, there would be sufficient data to be produced on the research.

---

[432]'Annual Report 2012' (*PT. Telekomunikasi Indonesia, Tbk.*, 2012) <http://www.telkom.co.id/download/File/UHI/2013/AR2012/TelkomAR2012.pdf> accessed 18 November 2014.
[433]Ibid.
[434]'Cloud Computing Infrastructure Technology - Telkomsigma' (*Telkomsigma*) <http://www.telkomsigma.co.id/cloud-computing/> accessed 22 January 2015.

Figure 1[435] shows the ICT company participants in the yellow boxes. PT Telkom is the parent company, with 52.6% shares held by the Indonesian government making PT Telkom subject to the regulation as a state-owned company.

This thesis will also highlight the organisational structure of PT Telkom as the parent company. The organisational structure of the company is important to seek the portion of training allocation to support the improvement of skill of ICT companies. The organisational structure of each company is different; depend on the size and the characteristics of the company. The diagram below will highlight the organisational structure of PT Telkom.

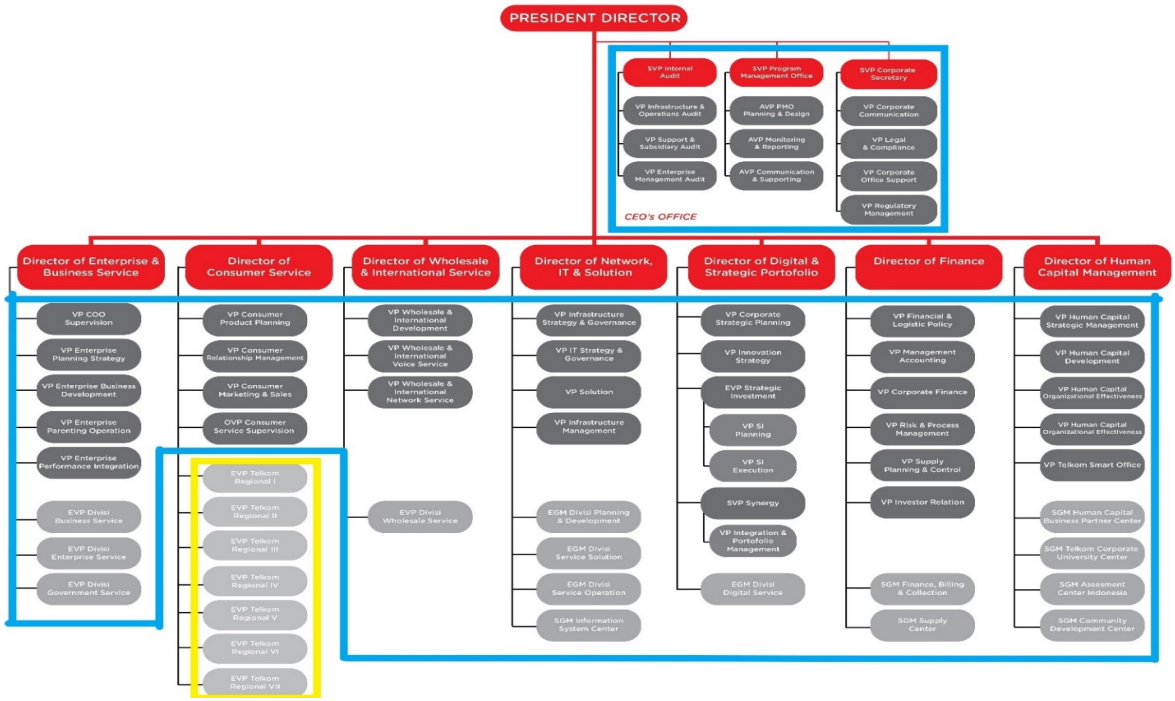

Figure 2. Telkom Organisation Structures

In Figure 2,[436] the yellow square indicates the division or regional office, while the blue square indicates the corporate office. The regional office is headed by an

[435]'Telkom Group Organisation Structure' (*Telkom.co.id*, 2018) <https://www.telkom.co.id/servlet/tk/mobile/about/en_US/companystructure/telkom-group-en.html> accessed 26 June 2018.
[436]'Telkom Group Organisation Structure' (*Telkom.co.id*, 2018) <https://www.telkom.co.id/servlet/tk/mobile/about/en_US/companystructure/company-structure.html> accessed 9 July 2018.

Executive Vice President (EVP) who is responsible to the divisional or regional office. The regional office's main responsibility is to market PT Telkom products. The corporate office is under supervision of the relevant Director. One of the responsibilities of the corporate office is to make a policy derived from the corporate strategy scenario (CSS).

3.3.2.2. Data analysis cycle

Data analysis is the most contentious cycle in the research. This is because the researcher should transform the data gathered from the data collection, identify it, and then put it into textual data analysis.[437] There are three approaches that can be used in analysis method, classical content analysis, discourse analysis and grounded theory.[438] In this research, researcher used classical content analysis. This method is used to examine and explore the result of the interviews from the interviewees in observation and document analysis.[439] The researcher used this method to examine the data from the interview transcripts.

Classical content analysis is used to analyse the phenomena arising from the legal cases or interview or policy. It might also consider the changing terms in case law.[440] In this research, the researcher used classical content analysis to reveal the phenomena in the Indonesian cloud computing industry that might affect the skills gaps in the company. Classical content analysis accommodated the data from company reports, legal cases and the company policy to confirm or reject the phenomena that is being studied. By using classical content analysis, the researcher will have a selective, valid and reliable result.[441]

Result from the interviews were taken from the person who directly deals with the policy in cloud computing and employee in the three biggest ICT companies in Indonesia which have used cloud computing as their business model. They were selected from all relevant personnel at the decision-making level. They are all in the

---

[437]Ibid. (n 410).
[438]Ibid. (n 411).
[439]Fred N Kerlinger, *Foundations of Behavioural Research* (2nd edn, Holt, Rinehart and Winston 1973).
[440]Ibid. (n 410).
[441]Ibid. (n 411).

position of the strategic managerial which related to the decision makers of the policy in the company. The interview results were added with the interpretation of the researcher to construct the code. In this research, the code could be selected from each term in the research, which are the growth of cloud computing, legal framework for employee protection, and data security and data protection. Each of these codes then summarised partly as specific as possible by analysing to what extent they are used, the limitation of those codes, how they affected, and so on. After the summarisation of the code, then it was labelled to categorise the data. This process is known as a coding frame.[442] Once codes are categorised, they can be related to seeking the relationship between those codes as the evidence of the research finding. The finding will determine either the codes based on the evidence will support the phenomena mentioned in the hypothesis or not.

In coding the code, the researcher initially used pen and paper. Computer was only used to collect and organise the data for coding. On the other hand, to construct the data for the code, analyse and reporting the findings of the research were still reliant on the interpretation and judgement of researcher.

3.3.2.3. Ethical issues

Ethical issues appear when doing research in social science that involves interaction with the human object. Conducting a qualitative method in research is leading to the purposes of getting perception, beliefs and experiences of the participants. However this method is often involving sensitive issues.[443] Therefore, having approval on ethical issues is important with a qualitative method. The researcher obtained clearance from Lancaster University's Ethics Committee on 29th September 2015, which allowed the researcher to carry out a series of semi-structured interviews as data collection.

Research can be categorised as a high-risk study if the research is studying in some illegal activities such as like when research is done in a situation where the subject is admitting a criminal or if the research is studying on in danger subjects that for

[442]Ibid. (n 411).
[443]Ibid. (n 410).

example including sexual offence that can danger the object of the research.[444] In such conditions, the researcher should obtain approval from the ethics committee before fieldwork is started.

One particular risk with this study comes from the possibility that the interviewee might disclose company information that may harm the company's reputation. However this is not the aim or focus of the research. The research does not consider sensitive areas in the company, and the company will not have access to the primary data. Both the researcher and PT Telkom fully understand that the aim of the research is to give an insight into the managerial skills that might arise from the growth of cloud computing in Indonesia. The research is fully supported by PT Telkom, to develop the researcher as a better employee and so to develop the performance of the company. For those reasons, PT Telkom is willing to support the project and was assured that the results will be used for educational purposes only.

There is also the possibility of revealing malpractice in the company. However, if any information was disclosed related to malpractice, it would not be disclosed unless the participant agrees. The interviewees were made aware of this through the participant information sheet. If the interviewee suspected any malpractice on confidentiality during the study, they could contact the Director of Postgraduate Studies (Research), Law School, Lancaster University School of Law to discuss the suspected malpractice. Disclosure related to the revealing of such condition was indicated on the participant information sheet. Therefore, as an employee, even though the research was to be conducted in the company which funded the research, however, the researcher was able to operate objectively. Moreover, the researcher was going to return to the position as an employee without prejudice. The interviews, which were conducted with eleven senior managers who have the authority to make a company policy related to cloud computing and employment, provided the actual insight into how they overcome the implementation of cloud computing. The results of the interview were then analysed with the existing policy and regulation of Indonesia and the UK.

---

[444]Ibid. (n 409).

Related to the findings of the research, as the research is fully supported by the company that has funded the researcher, it is important for the researcher to maintain objectivity towards the findings of the research. Given the area of study, the results and findings should support the company, not only in developing their performance, but also to address employee skills gaps.

3.4 Constraints on the Research Process

There are three main constraints to this study. The first is related to data collection. In data collection, the researcher deals with the difficulties of formulating the precise research questions to address the phenomena under study. Answering the research question is critical to comprehending the phenomena; therefore, it should portray the whole research project of the researcher. With the insight of the supervisor, the research questions are finally formed, and it can depict the project of the research. Another problem in data collection is integrating theory. Different jurisdictions of law require a researcher to make more effort in integrating theory in the civil and common law jurisdiction. There were a lot of cases and policy related to the research project; but not every case and policy was relevant. With the help of the computer software, the researcher sorted out the relevant cases and policy.

As the research was fully supported by the researcher's company, there were no concerns regarding financing the study.

3.5 Chapter Summary

This chapter has clarified the aims of the research, the methodology approach that is used to address the aims, ethical issues and constraints in doing the research by using a qualitative approach. The research is to analyse the relevant Indonesian, European Union as well as United Kingdom's policy and regulation. This research is to evaluate the relationship between the employees' skills and the phenomena that risen in the ICT companies, which is the implementation of the high level technology called cloud computing. Therefore, by using empirical legal research as a method will support researcher in legal findings of the research caused by the phenomena in the ICT industry. Researcher is elaborating the regulation and policy in United Kingdom in solving the problem arise from the growth of the technology related to the protection of the employee in the company. Classical content analysis will be used to examine

the semi-structured interview transcript which is collected through the data collection as well as data from legal documents and policy in employment to set a data in building the coding frame of the research. This chapter, in conclusion, is to look at the research validity and to develop a conceptual framework to answer the research question and to examine the hypothesis' accuracy of the research.

Next chapter will elaborate the analysis based on the interview held in the ICT companies. It will discuss the interview result from ICT companies as users as well as provider of cloud computing and it disclose the acceptance of cloud computing in the company. Comparison between EU, UK, and Indonesia's law is also state to make clear whether data security and data protection in cloud computing has already complied with Indonesian Law. This will come to result whether the law reform in Indonesian information related to data security and data protection could affect upon the cloud computing industry and affect the position of employees in Indonesian ICT companies.

Chapter 4. Data Analysis

4.1 The Interviews

From the interviews with the company policy makers, it can be seen how technology affects the policy-making process within a company. The interviews also highlight how businesses should be in line with the regulations in Indonesia. The policy makers are all individuals at the decision-making level, and their opinions are thus relevant to the subject matter.

This chapter will highlight how the participants were selected as individual relevant personnel at the decision-making level and in relevant companies. It will explain their important role in the company, especially related to the creation of policy documents, since their policy will be implemented and will have an impact on all the employees in the company.

4.1.1 Interviewees

The interviewees came from three ICT companies in Indonesia, PT Telekomunikasi Indonesia, Tbk. (Telkom Group), PT. Telekomunikasi Selular (Tsel), and TelkomSigma (see Section 3.3).

The first interviews were with Telkom Group. As a state-owned company, Telkom Group is subject to the State-owned Enterprises (SOEs) Law[445] and Limited Liability Companies Act.[446] It is also subject to regulation by the New York Stock Exchange and Indonesian Stock Exchange, since the company has listed on those stock exchanges.[447] Telkom Group has covered a complete range of telecommunication services, which includes cloud-based and server-based services. Telkom Group has numbers of subsidiaries that support its business services.

The second company, Tsel, is a Telkom Group subsidiary. As the widest-ranging mobile network operator in Indonesia, Tsel was the first to commercially operate the

---

[445] Indonesian Law 19/2003 regarding State-Owned Enterprises.
[446] Indonesian Act 40/2007 regarding Limited Liability Companies.
[447] 'Annual Report 2015' (*PT Telekomunikasi Indonesia, Tbk.*, 2016) <http://www.telkom.co.id/assets/uploads/2013/05/AR-TELKOM-2015_ENG.1.pdf> accessed 1 March 2017.

4G LTE technology that covered 14 key cities with 2.2 million users.[448] Tsel, as a subsidiary of Telkom Group, is subject to the Limited Liability Companies Act. However, even though Tsel is not subject to the SOE Law, in policy-making, Tsel has to consider the regulation that is implemented in Telkom Group as the parent company.

TelkomSigma is also a Telkom Group subsidiary, through which Telkom Group expanded its business in cloud services. TelkomSigma is a leading integrated end-to-end ICT solutions company in Indonesia.[449] Its services are consulting, managing IT, software, and data centre operation. It has provided cloud systems in Telkom Group and Tsel. Like Tsel, TelkomSigma is subject to the Limited Liability Companies Act, however, in policy-making, it should also consider regulations implemented within the Telkom Group.

Even though Telkom Group, Tsel, and TelkomSigma are connected, they stand on their own as individual companies with their own company policies; however, they must also refer their policy-making to the parent company and regulations that bind the parent company. Telkom Group is subject to the SOE Law, and although the Law does not apply specifically to the subsidiaries, they should refer to the regulation that applies to the parent company. Therefore, policy makers have to coordinate with each other, so they can be in line with the parent company's strategy and adjust their policy as individual companies and as subsidiaries, even though they have a different business specification. Therefore, this is interesting research since the researcher is interviewing policy makers of the company as a separate company and as a subsidiary company at the same time.

The data came from eleven interviews from the three companies. Initially there were twelve interviews but one of the interviews was cancelled as the subject had left the company, but the data collected from the eleven interviewees was sufficient to continue. They were all senior managers in the fields of human resources policy, technology development and policy, legal policy, and corporate social responsibility

---

[448]'Annual Report 2016' (*Telkomsel.com*, 2017) <https://www.telkomsel.com/en/about-us> accessed 28 August 2017.
[449]'About Us - Telkomsigma' (*Telkomsigma*, 2017) <http://www.telkomsigma.co.id/about-us/> accessed 28 August 2017.

policy. This makes this research into a unique research.

Participants were chosen by the Human Resources Director based on the interviewer participant information sheet and the consent sheet. During the interview process, some interviewees provided further information after the interview recording was stopped. This information was noted in a supplementary note to the interview.

The interviews took approximately one to one and a half hours. During the interview, participants were notified that the purpose of the research was for the enhancement of knowledge. The eleven participants agreed to take part in the interviews and gave the information to the best of their knowledge. Most of the participants gave informative answers so that the questions were relatively easy to develop, however, some participants were not enthusiastic and gave brief replies, so it was difficult to develop a question from their answers.

4.1.2 Interview results

The interview questions can be divided into 3 broad areas:

1. questions related to cloud and its implementation in the workplace;
2. questions on policy-making; and
3. questions on how policy has supported the development of employees' skills.

On questions related to cloud computing as technology, most participants were able to recognise the meaning of cloud computing, although in general, according to their perception, cloud computing was identified as data storage. The interviews revealed that all thepolicy makers believed that cloud was merely matter of data storage, even though 7 of the 11 saw this data storage as part of the new technology. In fact, the cloud is wider than just data storage (see Section 2.2.1), and comprehending this can give a different perspective in policy-making. A more in-depth knowledge of cloud computing is required not only for policy makers, but also for employees in order to run the business. EU Directive 2016/680[450] stated that, in electronic systems, there should be concern related to data security, personal data protection, processing by data controllers and data processors and supervisors.

[450]Ibid. (n 27), Article 1.3.

According to the policy makers, ICT employees are already aware of and implement cloud computingas data storage. The cloud in ICT companies was used as an intranet, an internet connection and data storage to keep the employees' data. ICT employees might use the intranet from a PC in the workplace or their own devices. The internet was accessed using employees' passwords. However, ICT employees need to understand the security in PCs or their devices, because it contains the data of themselves, their companies or their customers.

A better awareness of the legal aspects of cloud computing can support policy makers in making policies, and they should consider things not only from the business perspective but also from the legal perspective. Especially in ICT companies, even though policy needs to be in line with the existing technology, it should also be in line with the legal aspects of protection. As stated by one interviewee:

> 'Therefore, our policy must be in line with the existing technology'. (A1, SM)

This comment was confirmed by 6 of the 11 participants, who believed that to support the company's sustainability, technology has become one of the main considerations of policy makers, especially for ICT companies. However, a problem will then arise when the legal aspects appear in the business, because the promulgation of regulations in Indonesia is slower than the development of technology or business.

On questions related to employees' skill, all the policy makers agreed that in ICT companies, the implementation of new technology is a must, and ICT employees should be able to keep up with up-to-date technology. They should know the technology, especially if it is being used in the company and sold as a service to their customers. As a consequence, policy makers agreed that employees should update their skills to implement the technology. The statement of supporting employees to improve their skills was made on the CSS and derived into a policy. This policy outlined the company's strategy and the company's support in achieving the goals; part of the policy was training programmes and guidance, as in the Personal Development Review (PDR), which included a skill development plan review, performance and reward review and clear and constructive feedback that could be applied in the workplace.

Employees should be reactive in improving their knowledge and skills related to the

implementation of new technology. Policy makers have issued some guidance for employees to help with skill development. As stated by one interviewee:

> 'We'll make some kind of pocket book, well, it doesn't necessarily have to be in the form of a book; it can be a soft copy. But the context is for his guidance when he works in T1 and what his duty is, to understand the company culture, the corporate culture, the core values, what is competency, the policy direction, it means that CSS [Corporate Strategic Scenario] will summarised it. It should not relate to company confidentiality, data history, at least if he aware about those things, he will understand what to do'. (A1, SM)

The quotation above shows that the company, through policy makers, has already given guidance for employees to improve themselves in the workplace, and has providedthe information needed to ensure that the employees will cope with the changes in the company. However, it is the employees' responsibility to update themselves and a corresponding obligation of the company to train them in the skills needed.

The policy related to the development of technology for employees is implied throughout the employment cycle, from recruitment to termination. This is because ICT companies need to align their strategy with the development of technology and the skill of employees.[451] The development of technology can either threaten unemployment, because the workers cannot find demand for their skill, or it could become complementary between technology and skills to create highly-skilled employees.[452] Technological literacy is the effect of the development of technology, especially for ICT companies and should be one of the requirements in the recruitment process and training policy.

Technology has changed the behaviour of companies, work atmosphere, individual performance, organisation of companies, business strategy and employee interaction[453] and also affected the employees in performing their jobs.[454] Therefore, employees should be able to adjust themselves to the environment changing as a result

---

[451]Mehmet Ugur and Arup Mitra, 'Technology Adoption and Employment in Less Developed Countries: A Mixed-Method Systematic Review' (2017) 96 World Development.
[452]Ibid. (n 84).
[453]Ibid. (n 93).
[454]Ibid. (n 94).

of technology.[455] The adjustment might cause acceptance or rejection.[456]

While basic knowledge of IT is obviously essential, it is also important to increase the level of security awareness.[457] The company issues guidance on security to prevent employees from committing cybercrime in the workplace and to make sure that employees comply with the protection of personal data.

The implementation of technology in the workplace brings benefits. As stated by one interviewee:

> 'Technology changes people's habit. We don't have to meet in person, if I have a meeting in …, and the meeting is only 1 hour, I prefer using video conference or Skype and stay in my office'. (A1, SM)

This quotation was confirmed by all of the policy makers, who agreed that using cloud computing in the workplace has simplified their work. It also reduces emissions from transportation that they would otherwise use to attend the meeting. Another benefit of the cloud is that they can reduce the use of paper in the workplace. Therefore, ICT companies have suggested the use of technology in the workplace to be implemented as routine.

4.2 Discussion

All the policy makers agreed that cloud computing has been used in the company and they found no difficulties in using the cloud in the work place. They emphasised that the use of the cloud for data storage did not interfere with their daily activities. However, they also agreed that when employees are working in an ICT company, they should be literate in the development of technology in the workplace, including cloud computing. This statement was emphasised by an interviewee:

> 'This is a business institution working in a telecommunication technology. If we work in the field of technology but we do not understand technology, we should be ashamed of ourselves'. (A2, SM)

---

[455]Ibid. (n 93).
[456]Peter Thompson and Jing Chen, 'Disagreements, Employee Spinoffs and the Choice of Technology' (2011) 14 Review of Economic Dynamics.
[457]Zoltán Nyikes, 'Digital Competence and the Safety Awareness Base on the Assessments Results of the Middle East-European Generations' (2018) 22 Procedia Manufacturing.

They explained that the cloud was currently used as a data storage system, with a specific password. Employees might use it anytime, anywhere, with certain authorisation. In addition, they stated that cloud computing had actually been known as an intranet, that is an internet system specifically made for the use of employees. Therefore, in terms of the implementation of the cloud in workplace, they found no difficulties to adapt to it. According to one interviewee:

> 'There was no significant impact. I mean, cloud computing itself is actually a server. A server which is used by many people at once, we are [already] used to it'. (C3, SM)

This quotation above was also confirmed by all of the policy makers in all the ICT companies. However, cloud computing is not just a matter of data storage (see Section 2.2.1). Teneyuca,[458] Stitilis and Malinauskaite,[459] Bodei,[460] Monteleone,[461] and Reese[462] agree that there are numbers of concerns related to cloud computing rather than its purpose simply as data storage. They all affirmed that the knowledge of user and provider, especially related to the protection of data security, personal data, and data maintenance by the cloud provider, are significant in cloud implementation.

The perspectives on how the policy makers perceive the cloud could influence the process of policy-making. This is important since the ICT companies are transforming their business strategies into a digital business, and there are a lot of legal aspects related to the implementation of new technology in the business. Policy makers should be aware that shifting into digital business will have the consequences in law which might not yet be regulated in Indonesia. Policy makers should be able to adjust business demand with the availability of law related to the development of this technology.

4.2.1 Data security

At the time when the interviews were conducted, there was no specific Indonesian regulation related to Information Security Management Systems (ISMS); however, in

---

[458]Ibid. (n 61).
[459]Ibid. (n 50), S.K. Chaulya and G.M. Prasad.
[460]Ibid. (n 63).
[461]Ibid. (n 64).
[462]Ibid. (n 54).

April 2016, the Ministry of Communication and Information Technology released the Ministerial Regulation 4/2016 which mandated the use of ISO/IEC 27001 as guidance the assessment of security.[463] ISO/IEC 27001 is business guidance for ICT companieson how they should manage the classification, labelling, handling and protection of records, and the privacy and protection of personal data.[464] It states that the documentation of information in each organisation is dependent on the size and type of the organisation, but similar protection should be afforded by all. Before the Regulation was issued, ICT companiesalready used ISO/IEC 27001 for their security systems.

Humphreys stated that:

> 'the aim of these procedures for information security is to ensure that all staff know what they should do to handle information in way that protects its confidentiality, integrity and availability, whether it is the processing storage and archiving distribution, copying or disposal of information'.[465]

He also stated that thereshould be adequate policy in the company related to the care of the sensitive data and data protection. Companies that achieved ISO certification should meet the requirement required by ISO/IEC 27001.

Since the Indonesian regulation had not been issued when the interviews took place, it waslogical for the companies to refer to the security specifications in the ISO. After the regulation was promulgated, it was stated that ISO/IEC 27001 should be used as guidance. Most of the interviewees said that they used the provisions on the Indonesian Standard for Industry (KBLI) and ISO/IEC 27001 for ISMS. To have a protection during the implementation period of the regulations, the policy makers approached the regulator for a solution. One interviewee, confirmed by other policy makers, stated that:

> 'If it is related to the regulation, we, in the legal division [in the company] have a sub division called regulation unit. This unit [responsibility] is to do some approach to Government related to the business that is not been regulated yet. The unit and Government will seek the solution, meanwhile we in the legal unit will figure the preventive solution that might arise [from the

[463]Ibid. (n 10), Article 1(2).
[464]Ibid. (n 115).
[465]Ibid. (n 41).

> implementation of technology] when there is no regulation in the business'. (B2, SM)

The policy maker had taken the initiative to approach the government to advance the regulation to cope with the growth of technology in the business, and policy makers looked for a solution so that the technology could be implemented. These actions were implemented in all the participant companies in this thesis to make sure that the development of new business complied with the regulation, and if the regulation had not been issued, policy makers would make sure that their policy would protect the customer and the business itself. Related to the ISMS, policy makers had taken the proper steps for their internal policy by referring to ISO/IEC 27001. Their statements on seeking solutions to prevent legal consequences during the implementation period werethe right judgement for the company. When issued, Ministry Regulation 4/2016 stated that all providers should obtain ISO/IEC 27001 certification.[466] This means that the policy was already in line with the regulation by implementing ISO/IEC 27001 as their security management system.

However, on implementation, the importance of the security system had less attention. One of the interviewees stated that:

> 'When the regulation says that [data centre should have located in Indonesia], it was [difficult, because it did] not support by good technical understanding, and the technical direction is not supported by regulations in terms of business, technical and regulation. There was no synchronicity. Unlike Indonesia, China is all clear about this. They wouldn't allow ad-coding. They have followed it, but China developed its own programme. They have Google China; the people are supported'. (B3, SM)

The quotation explained that lack of understanding of security systems among personnel and government support through regulation made the business not develop as it was planned. Ignorance of the importance of the security systems also played a role.

If there are some issues related to technology, such as a crash or inability to access the computer system, employees tended to rely on the IT department to handle the issues. The importance of security had not been a priority as they tend to pass the security of

---

[466]Ibid. (n 10), Article 7.

the network to the IT department. Indirectly, this leveraged the responsibility for data security completely to the IT division in the company. One of the interviewees stated that:

> 'We use a lot of assumptions and disclaimers [related to the technology]. It means that we simply draft [standard] contracts with cloud customers … and [we] are not responsible for the content. It means that everyone can fill in the data, but when there is a dispute, we must be responsible for it. So, what we deal with is more related to the [standard] contracts. However, in terms of specific IT, we have never addressed the issue'. (C2, M)

This comment indicates that it is the responsibility of the IT department to make sure that the technology product complies with the technological matters, including the security system and data protection. The other units are only responsible for non-technical aspects. This statement was made by a senior manager in a company which directly providesa cloud service. However, other senior managers in other companies agreed that, in terms of the security of the electronic system, policy makers were already aware that their company complied with the security guidance and although they trusted the IT unit to oversee security, they were aware that there was a system to guard the security system in the company:

> 'The issues that arise from cloud computing are related to IT. In IT unit, they have their own certification related to the system. It is called ISO, ISO 2007 if I'm not mistaken. They maintain the security system as well'. (B2, SM)

This interviewee stated that the company had complied with the cloud security certification. They stated that the IT division had the responsibility to handle any problems that arose from the implementation of the cloud in the workplace, since they had gained a certificate on the certain technology. The IT division should know the policy and procedures related to ISMS. The policy maker was aware that they had a security protection, but did not know the detail of the ISMS.

The interviewee stated that:

> 'In the legal policy, our recommendation is all things in Telkomsel premises, then Telkomsel must have control over it. We have the control over authorisation, we have the password, and the access should be only in the hands of a certain person. This is part of the certification in Telkomsel related to the IT security policy'. (B2, SM)

This statement showed that, even though some of the policy makers did not know the

exact policy and procedures of the ISMS, they were aware that there was protection for access and authorisation related to cloud computing in their premises.

The quotation on the IT security policy from the interviewee above refers to ISO/IEC 27001. Policy makers ensured that data security was provided by the company through certification of ISO/IEC 27001. If we look in detail at ISO itself, there are several considerations that the policy makers should be aware of concerning acceptable use policy, information handling policy and procedures, access control policy, procedures and processes, and human resources policies, procedures, and process.[467]

If we look at Kaufman[468] statement that providers of the cloud should make sure that they protect the confidentiality, integrity and availability of its consumer data, and make sure that their storage meets the minimum security requirements, including encryption, authorisation access and data backup. He then suggested to combine the industry policy with the NIST oversight related to cybersecurity to achieve effective protection for data security.

All the subject companies of this study met the requirement for the protection of data. However, awareness of the security system within the company has not been fully enforced by the policy makers. This could be seen in the uncertainty among policy makers of the security system in their company, and how they treated security on their premises. Most of the policy makers tended to refer to the IT department whenever there was something that related to the security system. This should be changed, especially for a company using technology which requires high levels of protection. It is the responsibility of all employees to be aware of and maintain the security system, not only the IT department, since the customers of ICT companies will demand the protection of their data. The ICT customers in this thesis are not only public users, but also other companies that use the services of cloud providers.

Jaatun[469] stated that specific protection is needed to cope with current technology.

---

[467]Ibid. (n 10).
[468]Ibid. (n 200), Lori M. Kaufman.
[469]Ibid. (n 263).

Cayirci[470] stated that ISO is not a specific security protection for cloud deployment, which needs expert knowledge to implement. However, the concern over finding the proper solution to the security system in the cloud has shown that security is crucial for business, security and privacy. Cayirci showed that having ISO as the regulation will risk delay to the implementation of new security protection, since ISO itself is continuing to develop with the new technology. The statement is also a reminder that security system will always develop along with the development of the technology, therefore there is a need for employees to keep up-to-date with the security system, especially in ICT companies. If we look to the Indonesian Regulation on ISMS, there is no specific consideration related to the classification of the security protection. It emphasises the consideration based on the principle of risk. The classification of the security protection is important to provide the right protection in the cloud.

If we look at Article 5(2) of EU Directive 2016/1148, there are two significant concern which are related to the operators of essential services[471] and the digital service provider.[472] The operator of essential services can be notified through the maintenance service of critical societal economic activities, how they rely on the network and information system, and how it would have significant effect on its failure, while the digital service provider is the legal person that provides a digital service that must identify and take technical and organisational measures to manage the risks of the network security and information system as offered in their service.[473] The operator of essential service in EU is similar with the categorising in the Indonesian Ministry Regulation.

Ministry Regulation 4/2016[474] categorised the electronic system based on the principle of risk. The regulation divided the electronic system into three part: strategic electronic system; high electronic system; and low electronic system. The regulation explained that strategic electronic system has the serious impact on public concern, public service, continuity of administration of the state and national defence and security. High electronic system failure impact will affect certain sector services or

---

[470]Ibid. (n 200), Erdal Cayirci et al.
[471]Ibid. (n 28), Article 5.
[472]Ibid. (n 28), Article 4 (6).
[473]Ibid. (n 28), Article 16.
[474]Ibid. (n 10), Article 4.

areas, while the low electronic system failure affect is aside from the strategic and high electronic system. However, the Regulation does not state the responsibility of the digital service provider to provide the security protection.

The EU Directive distinguishes between the user of the network and information system and the provider, while the Indonesian regulation does not specifically define the provider or operator of network and information system. The separation in the EU Directive has clarified the responsibility of the digital service provider to provide the service to the operator of essential services. Clear classification of the provider's liability will give certainty to each party as to their obligation, and who will be responsible for data security.

Indonesian regulations regarding ISMS has coped with data security in Indonesia, but the specific responsibility of the service provider has not been settled. ISO/IEC 27001 has been a requirement for the provider to conduct their business, however, it is necessary to have a specific implementation regulation that governs operator responsibility related to data security to specify the responsibilities and obligations of the provider in delivering a service network. The researcher agrees with the statements of Jaatun and Cayirci, that there should be a specific protection related to data security that should be updated continuously in linewith the development of technology. This up-to-date security protection would help the ICT industry to develop and perform their cloud business.

However, Indonesia has made progress in data security system by the establishment of the Indonesian Cyber Agency and National Encryption Agency[475] in May 2017. The spirit was re-organise and merge the Indonesian Encryption Agency with the Informatics Directory of the Ministry of Communication and Information Technology to ensure that government policies related to cyber security are properly implemented. The main role of this organisation is to implement the cyber security by optimising, promoting, and consolidating all the elements related to cyber security. It's functions are to formulate, implement, monitor and evaluate the policies related to cyber security, and theidentification, detection, protection, recovery, monitoring, evaluation,

[475]Ibid. (n 12).

control of e-commerce protection, coding, screening, cyber diplomacy, cyber crisis management centre, cyber contact centre, information centre, mitigation support, vulnerability recovery, cyber incidents and/or attacks, and to perform the national, regional and international cooperation in cyber security.[476] Therefore, the enactment of this Presidential Degree is principally to support the cyber security in the relation with the national security.

4.2.2 Data protection

The regulations in Indonesia cover the protection in the data confidentiality,[477] data centres,[478] data security[479] and jurisdiction.[480] Even though it is not specific to cloud computing, the regulation has covered the important data protection aspects in the cloud. As a derivative of the Indonesian Law 11/2008 and Government Regulation 82/2012 outline provisions for personal data, that is: 'a specific individual data are stored, treated, and keep confidentiality'. The provision on the Regulation has been implemented by ICT companies:

> 'Therefore, not everyone has to know. The cloud and data centre on a server are the same thing. However, the data centre in the server is private. It is our own. Only we can access it. On the other hand, data saved in the cloud means saving it in a server that is used together with others. We save it in the cloud; it means everyone can access it. There are layers of security. We can save it anywhere. Interface to the users, to the employee is no difference'. (C1, SM)

The quotation states that ICT companies have the power to control authorisation and passwords, and can determine who can access the data. The policy makers stated that the data placed in the cloud can be shared through several layers of security. However, it is crucial for policy makers to understand that data stored in the cloud might contain private and personal data that should not be shared without restriction.

In the Indonesian Public Information Disclosure Act 14/2008,[481] there are several clauses that prohibit disclosure of information which is personal, such as history and

---

[476]Ibid. (n 12), Article 3.
[477]Ibid. (n 253), Article 15, 22.
[478]Ibid. (n 253), Article 17.
[479]Ibid. (n 253), Article 12 (1b), 19.
[480]Ibid. (n 253), Article 17.
[481] Indonesian Act 14/2008 regarding Public Information Disclosure, Article 17(h).

condition of a family, medical treatment, individual financial conditions, evaluation results and recommendation of capability, and personal notes of an individual related to educational activities; it thus protects personal data. However, it is contradictive of the provision of Article 15(3) of Government Regulation 82/2012, which states that there will be further explanation of personal data through ministerial regulation. The Regulation does not explain further the categories of specific individual data. Article 15(3) of the Regulation states that there will be further guidance for personal data in the form of Ministerial Regulation, but at the time of writing it had not been released.

The contradictions are that this Law is higher in the hierarchy than the Regulation. The hierarchy of Indonesian legislation according to Establishment of Legislation Act[482] is, in order: the constitution of Republic of Indonesia of 1945; followed by the Law or Government Regulation in Lieu of Law; Government Regulation; Presidential Regulation; and Regional Regulation. Therefore, the Government Regulation can only consider the Law. The second contradiction is related to the date of the establishment of the Regulation. The Law was established before the Regulation; therefore, the Law should be the government's position. Consequently, even though this law has the same definition of personal information, there should be further analysis if the personal information defined in Act 14/2008 is the same as in Government Regulation 82/2012.

In December 2016, the Minister of Communication and Information Technology finally promulgated the Personal-Data Protection within Electronic Systems Regulation[483] which regulated to what extent an organisation should protect personal data. It mandates the organisation to have an internal policy for processing personal data, but does not define it. Even so, this regulation places obligations on organisation to protect personal data from collection to erasure or destruction.

The UK's Data Protection Act 1998[484] states that certain categories of personal data should be protected. According to the Act, personal data is considered as data that can identify a person's identity if it is revealed. This Act has also defines sensitive personal data, that is personal data that consists of information such as racial or ethnic

---

[482] Indonesian Law 10/2004 regarding Establishment of Legislation, Article 7.
[483] Ibid. (n 11).
[484] Ibid. (n 278), Section 1(1).

origin, political opinions, beliefs, membership of a trade union, physical or mental condition, sex life, commission or alleged commission of any offence, and any proceedings for any offence committed. The DPA has regulated strict rules related to personal data.

In EU Directive 95/46/EC, personal data is defined as:

> 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.[485]

This definition was ratified through EU Regulation 2016/679[486] with the addition of the identifier of a name, location data, an online identifier, and genetic information. In this definition, the EU does not separate personal data and sensitive personal data. The EU makes specific mention that dealing with personal data should also include the sensitive data as explained in the DPA. The objective of having a clear definition is to have strict and precise protection of citizens'data, and give clear direction to the data controller and data processor regarding their responsibilities.

The company should be able to recognise the confidentiality of the data kept in their premises. According to Watson,[487] the partition applications in a cloud system should meet the security requirements. Jakimoski[488] stated that the cloud provider should make sure that they protect the data of their consumers through steps such as authentication, confidentiality, access control and authorisation. Therefore the company should know the degree of the data that should be protected and to what extent the data is being protected. It should be able to outline its responsibility for data protection, and consumers should be aware of their rights related to the data kept on the provider's premises. The imbalance of power between provider and user might lead to abusive practices, especially with sensitive data in the cloud and the cloud

---

[485]Ibid, (n 25), Article 2(a).
[486]Ibid. (n 26), Article 4(1).
[487]Ibid. (n 266).
[488]Kire Jakimoski, 'Security Techniques for Data Protection in Cloud Computing' (2016) 9 International Journal of Grid and Distributed Computing <http://dx.doi.org/10.14257/ijgdc.2016.9.1.05> accessed 4 November 2016.

service process.[489]

The legal certainty through the establishment of the Ministerial Regulation as a guidance for personal data will support the development of technology, especially for the cloud, since the protection of data is crucial in the cloud system. This regulation has regulated how personal data should be treated and managed by organisations. However, the category of personal data which should be protected is not specified the regulation;[490] but it states that there will be an introduction session for the public to deliver in-depth information related to the significance of personal data. Even though the government will organise education on the personal data, to give legal certainty, it is better to put a clear definition of personal data and its deliberation in the regulation to give Indonesia has a comprehensive regulation.

The Indonesia government could establish a national organisation to manage and control the implementation of data security and the protection of personal data,[491] like the national cyber security organisation supervised by the Ministry of Communication and Information Technology. The establishment of such a body, as proposed in this thesis, will ensure that electronic system operators fulfil the provisions of data protection principles. The organisation would be similar to the Working Party (WP) established by EU Directive 95/46/EC,[492] or the European Data Protection Board (EDPB) established under the EU General Data Protection Regulation 2016/679,[493] which are provide expert opinion on questions related to data protection, promote the uniform application of the general principles, give advice in processing personal data and privacy, and make recommendations to the public with regard to the processing of personal data.[494]

In the EU, the WP acts as the representative on behalf of data subjects, including industry. It has the responsibility to make sure that personal data protection is properly

---

[489]Ibid. (n 130), Konstantinos Stylianou, Jamila Venturini and Nicolo Zingales.
[490]Ibid. (n 11), Article 34.
[491] Hui Na Chua et al., 'Compliance to Personal Data Protection Principles: A Study of How Organisations Frame Privacy Policy Notices' (2017) 34 Telematics and Informatics.
[492]Ibid. (n 25), Articles 29 and 30.
[493]Ibid. (n 26), Article 68.
[494]'Tasks of the Article 29 Data Protection Working Party' (*European Union*, 2017) <http://ec.europa.eu/justice/data-protection/article-29/files/tasks-art-29_en.pdf> accessed 13 March 2017.

implemented. Experts aside from the WP might also participate and recommend ideas in supporting the enforcement of personal data protection. Article 29 of Directive 95/46/EC states that the WP should publish an annual report on personal data protection to indicate that EU has a commitment to provide the necessary protection. In EU Regulation 2016/679,[495] the EDPB is given an obligation to monitor and ensure that the regulation is applied correctly, giving advice and making recommendation related to implementation. It also has an obligation to publish an annual report related to implementation, including guidelines, recommendations and best practices regarding the protection of natural persons and processing in the EU and, where relevant, in third countries and international organisations.[496]

These provisions in Article 29 have been replicated in the Ministry Regulation,[497] which says that the government would provide any public information related to the implementation of personal data protection through the enactment of an organisation that is part of the Indonesian Ministry of Communication and Informatics.

EU Regulation 2016/679, which came into force on 25 May 2018, will change the role of the WP. It states that:[498]

> 'References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the EDPB established by this Regulation'.

EU Regulation 2016/679[499] states that a Data Protection Officer (DPO) will be designated to make sure that an organisation, including the data controller and data processor, provides sufficient protection for the personal data of data subjects. The designation of DPO is required, especially when the processing is carried out by the public authority, if the core activity of data controller or data processor is systematic and regular and on a large scale, or if the core activity of the data controller or data processor is on a large scale, processing special categories of data.[500] These are racial

---

[495]Ibid. (n 26), Article 70(1).
[496]Ibid. (n 26), Article 71.
[497]Ibid. (n 11), Article 34.
[498]Ibid. (n 26), Article 94(2).
[499]Ibid. (n 26), Article 37-39.
[500]Ibid. (n 26), Article 9.

or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic or biometric data for the purpose of identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, and personal data relating to criminal conviction.[501]

The DPO should meet the requirement of expertise in data protection law and practices, professional qualities, and the abilities to fulfil the tasks.[502] The DPO may be a staff member of the controller or processor;[503] however, they need to make sure that their tasksdo not result in a conflict of interests.[504]

The DPO has some specific tasks regarding to EU Regulation 2016/679, which are:

a. 'to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
b. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, understanding-raising and training of staff involved in processing operations, and the related audits;
c. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
d. to cooperate with the supervisory authority;
e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter'.[505]

The specific tasks of the WP or EDPB under the EU General Data Protection Regulation 2016/679,[506] and the DPO might help to elaborate on the requirement in the establishment of the Indonesian national organisation.

4.2.3 The roles of data controller and data processor

Regulation, for business continuity, should be able to protect all aspects of cloud computing. Indonesia has made regulations related to ISMS and the protection of

[501]Ibid. (n 26), Article 37(1).
[502]Ibid. (n 26), Article 37(5,6).
[503]Ibid. (n 26), Article 37(6).
[504]Ibid. (n 26), Article 38(6).
[505]Ibid. (n 26), Article 39.
[506]Ibid. (n 26), Article 68.

personal data in electronic systems. However, the Ministry Regulations do not define the roles of the data controller and data processor. To maintain data in Indonesia, the Indonesian government has a provision related to Electronic System Operators (ESO) in Government Regulation 82/2012, which refers to:

> 'any person, state administrator, business entity, and public that provides, manages, and/or operates an Electronic System, either individually or jointly, to the Electronic System users for the interests of its own and/or other parties'.[507]

Under this regulation, the ESO has duties on registration, hardware, software, experts, system management, the obligation to keep the personal data, good management and accountability, data and disaster recovery centres, security of the system and certification,[508] and 'shall maintain the confidentiality, integrity, and availability of the personal data are managed by ESO'.[509] Aside from that, the provisions in this regulation state that the ESO should make sure that the data kept are secure.

Indonesian Ministry Regulation 20/2016[510] regulates how personal data should be processed. The regulation states that personal data should be kept for five years. It states how the data should be kept, and how to delete data that is no longer needed. However, it does not state clearly who is in charge of the process.

Since there is no separation of data controller and data processor in the Indonesian regulations, companies in Indonesia that deal with electronic systems should meet the obligations of both data controller and data processor. The ICT companies' obligation is to specify and process the customers' personal data. The purpose of the regulation is not to separate the electronic system operators but to give comprehensive protection to the customer. However, itis stated in the regulation that the operator can delegate its obligation to an electronic agent through a specific contract.[511] This regulation can have a benefit or a disadvantage for the provider. The benefit is that the provider can give a comprehensive service and performance for its customers by being a one-stop shop. However, it will be a disadvantage for the provider if there is no separation

---

[507]Ibid. (n 253), Article 1 (4).
[508]Ibid. (n 253), Article 5-32.
[509]Ibid. (n 253), Article 15.
[510]Ibid. (n 11), Article 15-19, 25.
[511]Ibid. (n 253), Elucidation.

division in the company to handle the personal data. This will give legal uncertainty related to the responsibility of the maintenance of personal data. If the regulation has separated the obligations of the provider in relation to who will be responsible to the data controller or data processor, it will give clear protection for the provider and consumer in the light of personal data protection.

The UK's DPA distinguishes the terms of data controller and data processor and give clear separation of the responsibility of each. This separation is also enacted in the EU and is legally binding on its members, including the UK. Both the EU and the UK are very concerned about the protection of personal data. Therefore, this separation gives legal certainty for its members and companies that deal with personal data protection. The separation gives clarification of who owns the data and who will process it.

The DPA,[512] EU Directive 2016/680[513] and EU Regulation 2016/679[514] state clearly which legal person or public authority or agency or other body has a responsibility as data controller and data processor. In processing data, the separation of data controller and data processor could give a benefit in relation to the protection of personal data. According to the Information Commissioner's Office (ICO),[515] data processor activities are limited to the technical aspects of an operation, such as data storage, retrieval or erasure, while data controllers tend to the interpretation, professional judgement or decision-making in relation to personal data. In a cloud service, the cloud provider should determine whether they act as a data controller or data processor. This is important, since they have a responsibility to protect the user's personal data. Another benefit is that when a failure or breach on personal data occurs, it is relatively easy to see where the failure or breach is, and to look for a solution. EU Regulation 2016/679 states that data processing starts with several steps. Processing means:

> 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or

[512]Ibid. (n 278), Section 1(1).
[513]Ibid. (n 27), Article 3(8,9).
[514]Ibid. (n 26), Article 4(7,8).
[515]Ibid. (n 310).

otherwise making available, alignment or combination, restriction, erasure or destruction'.[516]

Article 6 explains to what extent personal data may be processed, including the approval of the data subject for compliance purposes. Personal data is highly respected by the EU regulation. In Article 24, it states that the controller has a responsibility for data protection and must take proper steps to make sure that they comply with the code of conduct. They also have to make sure that they fulfil the requirement of Article 40 and make it binding and enforceable through contractual or other binding instrument. The code of conduct mentioned in this article includes appropriate protection for personal data and the rights of the data subject. The controller and processor should prepare codes of conduct to comply with the regulation. This regulation was applicable in the year 2018. Since the regulation wascome into force on 25May 2018, the EU members have been given a transition time to adjust to the new EU regulation. The adjustment is stated on the regulation itself. Therefore, to comply with the law, it does not require any implementation regulation.

Referring back to the Indonesian Government Regulation 82/2012,[517] it is stated that the ESO should have procedures such as making a correction, confirming or reconfirming, and choose an activity. These protections also appear in Article 28 of Ministry Regulation 20/2016 on the responsibility of the ESO. Those protections are likely to have the same levels of protection that are offered in the new EU regulation, except there is no protection in the Indonesian regulation related to the protection ofchildren, notification of data breaches to data subjects, and the transfer of personal data to other countries.

Since the Regulation does not recognise separation between data controller and data processor, and if the company in Indonesia is to have the same level of protection of personal data as the EU and UK, we need to look further at the definition of data controller and data processor stated by EU regulation. In brief, data controllers are bodies that have the personal data, while data processors are bodies that have the

[516]Ibid. (n 26), Article 4(2).
[517]Ibid. (n 253), Article 26.

authority from the data controller to process the data.[518]

If we look at the participants in this thesis, first of all, we can take the example of Telkom Group as a stand-alone company. Assume that Telkom Group has its own IT system and can control its own employees' personal data. Telkom Group has mandated one of its division, for example the HR division, to process the employees' personal data. Therefore, Telkom Group can be categorised as the data controller, while the HR division is the data processor. However, since the IT system has been put in the cloud, and the cloudis maintained by TelkomSigma, the HR division is no longer the data processor. HR Telkom as part of Telkom Group has become the data controller, while TelkomSigma is the data processor. It should be realised by the employees in the Telkom Group that they have the right to make decisions related to personal data, and Telkom Sigma has the obligation to protect the personal data that is kept on its premises, related to the operational and technical aspects.

This is applicable to Tsel as well, since both Telkom Group and Tsel have delivered their employees' personal data to be maintained by TelkomSigma. However, the situation will be tricky for TelkomSigma, since they will become the data controller and the data processor at once, and they should have an internal policy to mandate which division will the data controller, and which will be the data processor. By the internal policy, employees will figure out their responsibility in the relation of personal data protection. Employees who have the authority to process the personal data should have a clearunderstanding of their responsibility.

The categorising of data processor and data controller in the EU regulation separates the responsibilities of employees in terms of data protection and they do not overlap. The confusion between rights and obligations of data controller and data processing can be avoided, and the company will perform its duties related to its type of service.

In the interviews, all the policy makers stated that Telkom Group and Tsel had delegated their data storage to TelkomSigma. TelkomSigma has the responsibility to perform, operate, maintain and protect the data of those companies. However, TelkomSigma outsourced its system to another vendor:

---

[518]Ibid. (n 26), Article 4(7), (8).

> ‘Meanwhile, the vendor as the owner of the technology should have the latest technology running. Our [TelkomSigma] position in the middle tries to integrate all, compare with the existing condition, and then review and plan’. (C3, SM)

As we can see from the quotation above, the policy maker stated that TelkomSigma did not own the cloud technology. This meant that even though the company had provided the cloud and its products, TelkomSigma still relied on another company to provide the system. TelkomSigma should inform their customers that they have delivered the system to another vendor, to meet the obligation of TelkomSigma as the cloud provider and to protect personal data.

If a company such as TelkomSigma delegates its system to another vendor, then it should be stated clearly in the contract that TelkomSigma is leveraging the responsibility of the data to the third party. There should be a detailed explanation of the responsibility that is borne by TelkomSigma and the responsibility that is borne by the third party. The cloud user, in this case, ICT companies and their employees, should be aware that their data is being transferred to another party. TelkomSigma need to make sure that the third party will protect the data and there is no breach of customer data. This condition has proved that it is necessary to have a differentiation between data processor and data controller.

If we look at *Court of Justice of the EU: C-362/14-Schrems*, the EU has explained that it is important for the user to understand the protection of personal data where is being stored. In that case, the data of users that been provided to Facebook Ireland should not be transferred and processed in another country without the consent of the user if the other country did not offer sufficient and adequate protection as the origin country, in this case the United States. The territorial (related to the multi jurisdictional aspects of the user and provider) issues are important for the ICT companies, especially in for the personal data protection, when the offering of goods or services, and when the payment of the data subject is required and the monitoring of their behaviour within the Union (as stated in Article 3 GDPR). Moreover, The EU affirms that transferring data to the third country should have an adequate and equivalent data protection in its domestic law or international commitments as stated in Article 45 GDPR.

This case opened a new perspective on how cloud providers have to make sure that users’ data kept on their premises is fully protected. If we refer to TelkomSigma in

Indonesia, they should inform their users if they delegate the cloud system to the third party. It is important for the customers of TelkomSigma to aware that their data is maintained not by TelkomSigma, but by another party. TelkomSigma customers should understand the consequences of the data being transferred to other party, as in the case of *Schrems*. It is the obligation of the data controller and data processor to maintain and protect the data of its user, especially personal data, and this should be clearly stated and protected by law.

The Indonesian regulation that integrates data controller and data processor as the ESO needs to be reconsidered, since all of the obligations of the operator are borne by the operator alone. The operator will need to make sure that they understand the responsibility in the cloud, especially in relation to data protection. Operators have to make sure that they have a clear consideration in the contract between user and provider related to the responsibility for personal data protection, and if the electronic system is being delegated to the third party, there should be consent from the user that their personal data will not be mistreated by the operator or the third party. This understanding should be forwarded to the employees of the company. They need to be aware of their obligation as an ESO and the new technology in the business.

4.2.4 Implementation of thecloud in the workplace

According to NIST,[519] the cloud can be considered technology related to networks, servers, storage, applications and services. It connects several important aspects, including technology, assets, human resources, compliance and commerce. The definition is explained as a cycle or ecosystem. One of the interviewees stated that:

> 'We, as the cloud provider, should have an ecosystem. The ecosystem is [consist of] us as [an] operational division, then we have sales team who work in the frontline, and also, we are supported by principles [management] and outdoor frame [regulation]. This is the ecosystem in which we try to update everybody. In other word, the sales should understand the market, that is, the trend needed by customers'. (C3, SM)

This quotation has a perspective that all divisions in the company should support each other by knowing about related technology. This perspective is also agreed by the

[519]Ibid. (n 46).

policy makers that have a technology background:

> 'My major [in the University] was technology, and I used to be the director of subsidiary on IT company. [Therefore] automatically, of course I will follow the future development of technology. For example, for communication, for data sharing, it [the cloud] helps a lot, we don't have to store data locally by ourselves. If we store locally, and there is a storage problem, the data will be lost. Now, that we have cloud computing, communication is faster, if we want to communicate with headquarter in Jakarta, for decision, it's no longer a problem'. (A1, SM)

The understanding of policy makers should be spread to all employees so they can build a healthy technology-based ecosystem. Employees should aware of and responsible for the data protection, data security, and confidentiality of the company's data and the employees' data themselves. One of the policy makers stated that:

> 'Actually, when we talk about cloud computing, we directed to security understanding when we input the data'. (A2, SM)

This statement shows that the policy maker is aware that they need to spread the understanding of data security in the company. EU Directive 97/66/EC[520] also states that companies in the telecommunication sectors should have appropriate technical and organisational procedures in place to provide for the security of their services. It states the importance for ICT companies to ensure that they have given adequate protection to the processing of personal data by ICT companies.[521] Therefore, policy makers should make sure that the employees are provided with an adequate understanding and knowledge related to the security system. To ensure this, at the beginning of every year, employees have to sign an online integrity pact to make sure that they did not breach the company's data and maintain confidentiality. In TelkomGroup, the integrity pact was issued in 2009.[522] This is one of the solutions for the company to maintain the company data and to comply with the auditing rules.

The integrity pact challenges the employees in the areas of integrity, business ethics, gratuities, insider trading, confidentiality and other actions that could directly or indirectly damage the company. This pact itself is a standard of security management

---

[520]Ibid. (n 253), Article 4(1).
[521]Ibid. (n 253), Article 1(1).
[522]Ibid. (n 447).

required in the Good Corporate Governance (GCG) provision. By signing the integrity pact, the company has given a lesson in understanding the security system in the workplace, although it is not clear if the result indicates the knowledge levels of the employees or is just a compulsary that should be done by the employees.

If we look at the human resources aspects, ISO/IEC 27001 highlighted the important role of employees. Humphreys[523] emphasised that the biggest threat to an information system comes from human error. His statement is strengthened with cases related to the misuse of computer and authorisation (see Chapter 2). Humphreys[524] further stated that: 'The organisation need to ensure that staff are aware of information security risks and have sufficient understanding to support the organisation's information security policy to undertake their normal work functions and tasks. Staff should be trained in the use of information security policies and procedures, security controls applicable to their job function and the correct use of IT (e.g., log in procedures, keeping passwords safe, appropriate use of IT)'. If we look at Humphreys' statement, it is in line with the statement form the interviewees that there should be an ecosystem to update the employees related to the development of technology. This includes the issues and risksinvolved in the technology, and shows the need for continuous education for employees. Kizza[525] explained that cybercrime is an illegal action involving computer system as an object, a tool to commit a crime, or an evidence of a crime (see Chapter 2). This includes breaking into a telecommunication network without authorised access. He stated that insiders, hackers, criminal groups, disgruntled ex-employees and economic spies have been identified as sources of cybercrime. Kizza said that employees could have great potential to become cybercriminals since they have authority to access the system, and that most of the cases in the technology and telecommunication sector were committed by the employees themselves. Therefore, to minimise the potential of cybercrime in the workplace, it is crucial for the company to make sure that their employees has been provided withan integrity agreement, as done by Telkom Group through its integrity pact.

To have a comprehensive understanding, policy makers should realise their

[523]Ibid. (n 41).
[524]Ibid. (n 41).
[525]Ibid. (n 37).

responsibility to develop a policy that could improve the knowledge of the employees, especially related to data protection in the workplace, which not only involves the employees' data, but the company's and the customers' data as well. Recognising the potential crime that might occur by employees might support the policy makers in making a policy that can reduce cybercrime.

The UK's Computer Misuse Act (CMA) 1990 covers unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences, and unauthorised modification of computer material.[526] It gives legal certainty on the use of a computer. In relation to the cloud in ICT companies, providers need to make sure that users'personal data is safe and properly kept. This is to avoid the intentional (such as data breach by an employee) or unintentional (such as deletion of files or information) errors that occasionally happen.[527] In the development of computer technology, it is necessary to have a regulation that closely monitors the computer system. If we look at Indonesia regulation, there are no specific regulations that deal with people who breach the computer data security. In the workplace, they only use company policy and ISO as a security procedure. A breach in the company merely results in disciplinary procedure and dismissal, but the impact of the data breach can affect reputation and stock price.[528] Therefore, it is important for the employee to know and understand their responsibility related to the protection of data. If we refer to ISO/IEC 27001, the company should pay more attention to increasing the understanding of its employees on information security, management commitment and leadership across the life-cycle of employment.[529]

In the recruitment cycle, the human resource team should be able to identify the right people for the right job. The policy makers in ICT companies state the company's direction and needs. They recruit a person who has a capability required by the company, a professional or recent graduate.

---

[526]Ibid. (n 292), Section 1-3.
[527]Ibid. (n 115).
[528]Alessandro Acquisti, Allan Friedman and Rahul Telang, 'Is There a Cost to Privacy Breaches? An Event Study', *International Conference on Information Systems* (2006) <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf> accessed 1 September 2016.
[529]Ibid. (n 41).

The Corporate Strategic Scenario (CSS) consists of the corporate's short- and long-term plan and is approved by the board of directors. It is reviewed annually to look for any business fluctuations and strategy. The plan is not merely for the business, but also how the management supports the business, and this includes the policy on recruitment, training and termination of employees, either professional or recent graduate. The recruiting process in smaller companies is different. The smaller sized company tends to recruit established professionals. They need experienced and expert people without a need to provide specific training. One of the interviewees stated that:

> 'We never have such a massive recruitment. Ours is based on needs. Here in Sigma we have two divisions: project and service management. The project division could have recruitment (people) if it doesn't have any personnel [qualified]. However, in service management it is based on our [business] plan'. (C1, SM)

This shows that ICT companies are no longer recruiting huge numbers of employees, but they recruit specific people with knowledge of the technology. Since not all employees have adequate capability in the new technology, the decision to hire a professional for a certain period has become one of the fastest solutions to address the lack of employee competence. As one interviewee put it:

> 'We are not neglecting the spirit that digital itself is the consumption of the youth… Meanwhile it is not possible for us to learn how to play with a gadget, the older generation like me cannot keep up, reading gadgets, and it is tiring. The digital content, the subscribers are mostly from younger generation, it is absurd if the provider is some people from older generation that is not suitable. Now, in relation to that, no other way, we need to hire younger employees, not necessarily fresh graduates. I will propose actually, to hire people from digital [experienced people].... But now, why not if there is someone who is professional hire with the age around 30, let's say an ex-employee of Gojek or Twitter Indonesia or leasing Yahoo Indonesia. They know more about digital business, we will accept them'. (A1, SM)

This explains that ICT companies are tending to hire people who are digital-literate to support their business strategy. For the short solution to the implementation of technology, policy makers tend to hire people with adequate knowledge and experience. The interviewee went on:

> 'Our [company] direction is towards digital business and international business…, we have to manage the policy. And when we want to recruit people for the digital business, we need to understand the specification that we need to enter the digital business'. (A1, SM)

Based on the interviews, the policy makers stated that the development of technology had become one of the reasonsfor recruitment. Policy makers should refer to the CSS that has been approved and ratified by the directors. In ICT it is important to include a policy related to the development of technology to support the digital business. Therefore, technology literacy become a consideration in policy-making related to recruitment. This is an improvement in the recruitment system in ICT companies, since nowadays people are more literate in technology. Therefore, ICT employees should be one step ahead in becoming a leading company, especially for ICT companies. The policy makers focused on a digital perspective when it comes to hiring people:

> 'And when we want to recruit people for the digital business, we need to understand the specifications to enter the digital business. … to find staff for digital business now is different from before. We were, in Telkom, used to recruit people with high GPA, more than 3 GPA. Now we compare our methods with Google, Facebook, and the others, and we learnt how they recruit person. They have several criteria, for example creativity. That is clear, high GPA does not guarantee people will be suitable in digital business, and this will give an insight for our company. Therefore, we do not have to talk about the strict requirement for high GPA.… Now, maybe we start to ask for average GPA, not too high, we lower it, to get people with lower GPA that maybe suitable to work with us. The most important thing is, secondly, when we see how Google recruits people, it turned out that they only use interviews; they call it some kind of situational interview, there were also behavioural interview and others. Now, in the future, we will try to adopt their method of recruiting. So, if our interview previously was formative, like some kind of normative, because we need people with high GPA, now we are no longer need that, now we even asked some uncommon questions. Like in Google for example, I once read on the discussion forum how Google asked interviewees uncommon questions … It turned out that they wanted to see a creative answer. People who are normative usually cannot answer, right? How do you answer that? we do not know, but for people who are, like an open the box, they had the answer. Now, that was the example, we need to have one point in our CSS, that we see our business in the future, what we want, we benchmark companies with good performance in how they work. We need to observe closely to what we want to compare with'. (A1, SM)

This shows that the interviewee has looked for a solution to comply with the provision in the CSS by including some new criteria on their recruitment policy to support the digital business .The recruitment referred to is the recruitment of fresh graduates to fill the regular employment and professional recruitment to fill the skills gaps in the company.

However, hiring a professional has its own consequences. One of the positives is that they do not need to train people, and one of the negatives is there might be resistance from existing employees:

> 'At first the employee will surely reject it; they disagree if we do professional hire … for the [existing] employee who starts from the beginning and then suddenly there is a new person in a higher position [and they feel threatened]'. (A1, SM)

However, policy makers make their own judgement when they want to hire a professional. Lack of knowledge and skill of the employees has become the background of professional recruitment. However, to address the concern of the current employees in the company, it can organise training programmes to improve the skill of the employees. Training can be used as a tool in the organisation to improve the skill and knowledge of the employees.[530]As stated by one interviewee:

> 'There are … training, … that were competence specific or technical, technical is related to the line of work, for marketing, the training will be about marketing, for operational the training will be about operational'. (A1, SM)

This shows that the company can has also accommodate the employees' necessity to improve their skill.The training policy in the company is mentioned as a non-cash benefit for employees. Employees have a right to propose training,[531] however, not every proposal has been approved by the company. There are several considerations made by the HR department before approving training. As one of the interviewees stated that:

> 'Usually, the company can decline the [training] request. I happened to be rejected once [when I requested for a training]. It all depends on the availability of budget. Then, it depends on whether the company needs it, and whether the supervisor approves or not. In the end, it all depends on the company's programmes'. (A2, SM)

As we can see from the quotation above, the training is not merely dependent on the budget, but also the approval from the supervisor, and whether it is in line with the

---

[530]Jalal Hanaysha, 'Examining the Effects of Employee Empowerment, Teamwork, And Employee Training on Organisational Commitment' (2016) 229 Procedia - Social and Behavioural Sciences.
[531]Ibid. (n 39), Article 11.

company's strategy. This could be a problem when the company has many employees and is distributed in various regions, like Telkom Group and Tsel. As stated by one of the interviewees:

> 'The training is not yet structured. Therefore, it means that it all depends on the supervisor's consideration. For example, they will take turns… For example, if we have three or six staff, two of them will join the training this year and next year, two others will join the training. Therefore, it is still manual and unstructured…In the unit, it depends on the supervisors. Maybe many things are overloaded as well, such as the seniority and competence of the … officials [employee] in the local areas'. (A2, SM)

The quotation shows that attending training is determined by the supervisor and whether there is an opportunity to leave work, since the workload in branch offices is relatively high compared to the corporate office. Therefore, the opportunities for branch office employees in rural regions to access training are fewer than at headquarters. There are several steps before the training proposal is approved. It starts with the appraisal of the performance and competence of the employees, followed by a recommendation from their supervisor. The supervisor will then follow up the proposal to the human resource division. The human resource division will look for the budget and the necessity of the division and the company. The interviewees stated that a training proposal that will be rejected if there is a shortage in the budgetin the Annual Business and Budget Plan. Article 1(10) of the Indonesian Manpower Act[532] states that job/ work competence is 'the ability of each individu to work in aspecs such knowledge, skill and work attitude in accordance with established standard'. This act is translated by the policy makers in the company with the same manner. According to one interviewee:

> 'There are two [type of] trainings. First, leadership training, that is managerial and there are others that were competence specific or technical, technical is related to the line of work'. (A1, SM)

The quotation above states that company has helped the employees to improve their skill, not only related to their job, but to leadership. However, if we look further in

[532]Ibid. (n 39), Article 1(10).

ISO/IEC 27001,[533] it is stated that the objective of the training should include awareness of the information security and risks, policies and procedures, and skills for career development. It is important for employees to understand their risk in the workplace, so they can avoid getting involved in civil or criminal activities that include personal data. If we look back again in the statements of the policymakers in the light of their understanding of the cloud, they are assumed to have a narrow understanding of cloud data storage and everything that can be put in that data storage including email and information related to the workplace. Even though their perception is acceptable, the cloud is more than just data storage. The statements show that information security training is likely intended for technical employees, since the training is given according to the role, whereas, in ICT companies, all employees, according to ISO/IEC 27001 should be given training or an introduction to information security.

ISO/IEC 27001 also stated that there is more provision related to the use of cloudservices that need to be considered, especially in information security. This is crucial for cloud service providers given the data that they hold. An example of protecting employee's data is by considering the lawfulness of reading the content of employees' personal email.[534] With the growth of technology and the workload in the workplace, employees tend to skip the important meaning of data protection and rely on the IT division. Therefore, policy makers should build the understanding of the importance of personal data protection. This could be through briefing from senior management or through continuous training or through the online signing of an integrity pact.

However, not every policy maker realised this position. Previous statements from other policy makers said that only the IT division needed to deepen their knowledge of technology, because the impact of that statement affects how the policy makers make their judgement on improving the knowledge of employees other than from the IT division. One of the interviewees stated that:

---

[533]Ibid. (n 115).
[534]Franziska Boehm, Tim Hey and Robert Ortner, 'How to Measure IT Security Awareness of Employees: A Comparison to E-Mail Surveillance at The Workplace' (2016) 7 European Journal of Law and Technology <http://ejlt.org/article/view/500/634> accessed 2 September 2016.

> 'The technical people [IT division] are [being] prioritised [by the Human Resource Division] to attend trainings. It means that the trainings are intended primarily for people who are dealt with technical matters. [Therefore] Because the legal unit is a supporting unit, not the core unit, that makes we become the second or third priority [to have and attend the training]'. (C2, M)

This statement has created a barrier. He or she has made his or her own silo in the company that can lead to the lack of opportunity for him to improve his skill. That statement was also confirmed by another policy maker at senior managerial level in the same company, that stated:

> 'So other units [in the company] that do not have to use the cloud don't have to understand it, because it is different. Because the cloud and data centreare almost the same. The difference is the users. So, a sales person doesn't have to know [in detail] about the cloud. Support[-ing] staff only [need to] knows what the cloud business is like'. (C3, SM)

The supporting division refers to a division that does not make a direct contribution to the company's revenue. According to Kaplan, the function of support unit is to support the strategies and plans of each strategic business unit.[535] An interesting point of view from the interviewees is that supporting units only need to know a little about the technology. However, a support division such as the legal department should assess the consequences of the implementation of technology. The understanding of the company's strategy in the workplace should be spread to all employees.[536] The process starts with education to create awareness throughout the organisation. Therefore, it is important for all employees to be aware and understand the impact of the implementation of technology and not only exclusively for certain units that are related to technology.

Kaplan[537] also argues that silos between divisions and units in a company should be eliminated to support the development of the company. Raising organisational understanding and communication between the divisions and generating team spirit

---

[535]Robert S Kaplan and David P Norton, *the Strategy-Focused Organisation* (Harvard Business School Press 2001).
[536]Ibid.
[537]Ibid. (n 533).

might reduce silos in the company.[538] This effort will also to support the success of the company's strategy. Communication between policy makers and employees will create a positive environment in the workplace and to support change in the company,[539] including the implementation of new technology such ascloud computing. The eagerness of employees and policy makers to understand the cloud will support the business and help improve the skill of the employees.

If we look back at the interview results, all the participants seemed to see the benefit of using the cloud, which allowed them to work remotelyand simplified the work. Employees no longer needed to have a face-to-face meeting. All the policy makers thought that the cloud could help to reduce the time they spent attending meetings. They could video conference or hold a virtual meeting and put the meeting materials in a specific data store, with a password that only certain related employees could access. It is a risk for a company if the policy makers do not understand the core of its policy, for example if the policy-maker does not know the regulations in the cloud. If we look atthe statement of the interviewee:

> 'In terms of specific IT, we have never addressed the issue whether this product is lawful [according to the Indonesian law] or not. In terms of regulations, I admit, we are not updated with the latest information on IT. As far as I know, there are no specific regulations on data centres and how the data centres must be run' (C2, M)

This statement suggests that the interviewee has a lack of understanding of technology, either the technology as a service product or the legal consequence of the implementation of the technology itself. He also explained that the legal division is merely supporting the business through a cloud contract, which is an agreement of both provider and user in terms of the services of the cloud. Other than the agreement, it is the domain of other divisions. This cannot be justified, since as senior management in the company, he should look for a solution and should update himself on the newest regulation, so that he can support the business. The regulations in this thesis are either related to the technology itself or regulation related to the impact of

---

[538]Oachesu Madalina, 'Conflict Management, A New Challenge' (2016) 39 Procedia Economics and Finance.
[539]By Roland Bel, Vladimir Smirnov and Andrew Wait, 'Managing Change: Communication, Managerial Style and Change in Organisations' (2018) 69 Economic Modelling.

the implementation of regulation, such as regulation related to data security or data protection. He, as senior management, should also look for any approach to the govermnent to find the best solution if the regulation has not been finalised yet. He, as the leader, should encourage his team to take part in the ecosystem in the workplace by maximising the facility from the company, such as through peer-to-peer department sharing or training.

The consideration of taking part in the training programme depends on how effective the training impact on the business is. If we look back at the terms in ISO/IEC 27001, training should be given according to job function, thus it should be related to the daily work of the employees. One of the interviewees explained that:

> 'If we look at the number [of training], mostly [training is related to] technical [in line with the job position]. Well, of course still technical [related to daily work]. … From the leadership [training] side, that is not so much, I mean by the number of participants. Because the employee [that has been selected] for leadership [training] is only 20 percent of the rest [employees with performed capacity and prepare to be a leader]… The career committee will choose 20% of all employee, from all level, that we consider having the talent and to those 20% we will be given a leadership training, we call these 20% group as the talent group or talent pool. So, let's say our employees are 15,000 – 16,000, we select 20% across all levels to get a leadership training... And we did not ignore the 80%, we develop them, but in different treatment. To clarify it, let's just say that the leadership training is about managerial and leadership'. (A1, SM)

This suggests that the company provides an adequate proportion of people to attend training based on the employees' job. He or she stated that he or she has already allocated 80% of the employees to attend training relevant to their job, and that 20% of the most able employees have the opportunity to become a leader. This allocation has shown that management wants to improve the skill of its employees, whether related to their role or to their career path.

To support the business, it is important for employees to have the skills required by the company in the light of the company strategy. 'Strengthening education and skills is an important policy lever for development'.[540] It is the concern of the Human

[540]Rupert Maclean and Shanti Jagannathan, *Skills Development for Inclusive and Sustainable Growth in Developing Asia-Pacific* (Springer 2013).

Resource division to balance the needs of the company with the eagerness of employees in training, especially technical training. Even though it is important to improve the skills of employees, their improvement should benefit the company. This provision is reflected in the CSS and in how policy makers made their policy. Therefore, as stated by A1 SM, training given to employees will be adjusted according to their line of work. However, employees still can propose training aside from their line of work as long asit supports their assignment and is in line with business transformation in the company.

There are a lot of reasons why there should be a transformation in business in the company. One of them might be related to the development of technology, and all of the company's strategy is stated in the CSS. As stated by one interviewee:

> '…we have Corporate Subject Scenario [CSS], it has the company' vision and mission. It detailed the programmes for each directorate. We call it …strategic plan. …we have to be in line with it. If for example it was mentioned that the direction of business will be digital business, then our policy must support it. It means that we have to make policy to that direction. The simplest example, we have what we call the competence directory or competence library. The directorate is formed to measure people competence. … I have to develop competency directory to support digital business…we'll make some kind of pocket book … the context is for his guidance when he works in Telkom and what his duty is, to understand the company culture, the corporate culture, the core values, what is competency, the policy direction... It should not relate to company confidentiality, data history'. (A1, SM)

This statement shows that the company strategy is stated in the CSS document, and all employees have access to the document. The CSS itself had already been ratified by the directors and then cascaded to each division through the policy makers to adapt to the new CSS in policy-making. This process then tied leaders in each division to make an adjustment related to transformation, including adjustment of training to support the company strategy.

According to A1 SM, ICT companies in Indonesia are transforming into digital and international businesses. Therefore, it is important for the policy makers to base their policy on the newest technology and also technology that is recognised internationally. It is obvious that technical training in ICT companies will be the most preferable for the policy makers, especially in the HR department to organise training that is related to supporting the business.

In ICT companies, it is important to align the policy with the business perspective. The ICT companies' strategic planning is to become a leader of digital innovation in Indonesia. Therefore, it is important for them to transform the human resources, culture and organisation to achieve the goal.[541] It means that in policy-making, policy makers should support the company's business strategy by aligning their policy to support digitalisation. Employees should become digitally literate; not only for the existing employees, butalso in the recruitment process for new employees. Policy makers realise that it takes time to educate all the employees, especially if the company has a large workforce like Telkom Group. In accordance with the company's business strategy, in the recruitment process, policy makers should give consideration toa digital understanding qualification. For existing employees, policy makers should make some policies related to improving skills to deal with the implementation of technology, for example by making policy in digital understanding training, data security standard qualification and data protection training. This policy is made to support the development of ICT business in Indonesia:

> 'Business or technology. Since we are an IT company, so technology is what we sell. …. we build something based on the new technology available. But we must consider whether the technology suits the Indonesian market or not. We must consider other technology which is more suitable and more efficient with the condition in Indonesia'. (A2, SM)

This shows that policy makers should consider whether the development of technology is applicable in Indonesia. To understand whether or not it is, it could be obtained through a Personal Development Review (PDR) in the training process where an employee can make an input the performance and development plan, which could support the implementation of new technology.

However, the implementation of new technology in Indonesia is not merely related to the readiness of technological aspect, but also to the readiness of legal aspect of the implementation of technology. The development of technology generates new opportunity for law enforcement.[542] Therefore, it is important for the policy makers to recognise the impact of the technology on the market, both technological and legal. In

---

[541]Norma Riccucci, *Public Personnel Management* (5th edn, 2015).
[542]Ibid. (n 376).

using the technology, ICT companies should be based on lawfulness. The technology should have legal certainty and companies should know the impact of the implementation.

If we look back on the previous statement on the obstacles to the implementation of the cloud, the skill of the employees and lack of regulation are the most considerable for ICT companies. While the policy makers are making efforts to effect a transformation in human resources, culture and organisation, often lack of regulation becomes a barrier in executing the policy.

However, not all employees are eager to see the implementation of new technology. Their unwillingness to receive and implement the new technology might be a barrier for companies to move forward. To overcome this problem, policy makers have made policy related to people who not be able to follow the development of technology. It called the exit system. In ICT companies, there are two types of the exit system:

> 'So, I am making a policy called exit system. It is something called APS. APS is early retirement, retirement based on self-request, … Now, there are two types in exit system, normal retirement based on self-request or because of dismiss, but the number of dismiss employees are small because it is related to the employee's offense. [therefore] I make addition on the exit system, for example golden handshake. We had implemented it and around 600 are already retired. However, that is not enough, because if we want to turn the [age] pyramid upside down, for the 77% percent, it will need a huge effort and with recruitment of new employee and pushing older employee to retire will take more than 10 years... we also have silver handshake, to help the effort a little bit. It means that Telkom's employees were asked to be transferred to Telkom's subsidiary and the salary will be adjusted to the subsidiary level, which is lower, and we will give compensation although not as big as golden handshake. … will be adjusted to the subsidiary level, that one addition beside golden handshake'. (A1, SM)

This shows that golden and silver handshake exit system scheme represent compliance with the application of the law by not sacking but incentivising withdraw from the employment pool. It is of course at first the policy makers should comply with the clause in the Indonesia Act of Manpower by not dismissing employees due to the lack of competence, however, as a business entity, policy makers should also consider the requirement in the company to support the company's business strategy. Therefore, incentivising the employee would be the best solution for the company and employee.

Those exit systems answer the needs of the companies to recruit younger people,

which is in line with the company's business strategy:

> '…. in the digital business we need younger generation. It is like this, for example, like me, I still have time 6-7 years before retirement, there are plenty employees like me at the upper level. It is hard to manage them, while the higher the level, the less position is available. What are we going to do? With the new system, we asked him to have silver handshake, we shift him to our subsidiary for 3-year minimum. It is like regular silver handshake but only three years. For the regular silver handshake, let's say he is 45 years old, then he still has 10 working year in the subsidiary. But not this one, generic silver handshake, I call it special silver eject, he is offered three years to work with Telkom, that is minimum, can be extended if still needed. So, the status of the employee is not as permanent employee, but on project based'. (A1, SM)

This shows that, aside from the lack of skill, age can also become a factor so exit systems are suitable to be implemented for ICT companies in Indonesia. According to CSS, ICT companies require younger people to deliver the company's business strategy. The interviewee assumed that younger people have more to contribute to the company's strategy. Therefore, they made a policy to offer people over 45 the exit system. This is contradictive of the research by Riszuto,[543] which found that older workers were more willing to accept the implementation of new technology. However, even though policy makers believe that, to succeed in the digital business, the company will need people with adequate skill and competence, the interviewee has already accommodated employees that who cannot keep up with the implementation of new technology. It is more to be done to improve training, not only to add more numbers of training but also the quality of the training.

Policy maker are required to think more how to improve the opportunity of the employee in the rural locations to have more training, as well as to employees over the age of 45, since they are still the become the company's responsibility to improve the skill and knowledge. However, policy maker should notice that employee over 45 years might have different motivations or skill that need to be considered in the training.[544] Therefore, policy makers should look for solution to overcome the lack of

---

[543]Tracey E. Riszuto, 'Age and Technology Innovation in the Workplace: Does Work Context Matter?' (2011) 27 Computers in Human Behaviour.
[544] Bernhard Boockmann, Jan Fries and Christian Göbel, 'Specific Measures For Older Employees And Late Career Employment' (2018) 12 The Journal of the Economics of Ageing.

training in those areas.

The interviewee stated that making policy to appreciate current employees is welcome and acceptable by the employees, rather than dismissing them:

> 'I did some survey before I make a policy for the band first position, for the professional hire, I made a survey for band position 1 and 2, there are 800 something employees, the one who filled out the form are 261, and it is about 35%. From the survey point of view, it was already above 30%. So, 261 from 82% stated that they agree with professional hire, it means that they are aware that the business is belong to the youth, so they have a second thought not to retire at the age of 56. Further, Band 1 and 2,82% agreed, while 18% percent said disagree, but it is normal to have pro and contra. From the 82,81% agree with the transition, however, there's an input for band position 1 that they want to have another chance in the company before signing the contract, working for one year and then sign contract, they aware that this is not his era anymore. It is not fair if we asked him to resign with little compensation benefit. So, if we asked him to retire early, we have to provide fair compensation benefit'. (A1, SM)

This quotation shows that, before making a policy, the policy maker should include the opinion of the employee to provide acceptance of the policy. An exit system with fair compensation not only gives a benefit to the company by decreasing the number of employees, but also to the employee to look for another opportunity due to a lack of skill or the age factor.

The Act of Manpower states that an employee should not be dismissed for incompetence and that companies should make some effort to avoid a dismissal. The Act then explains on what grounds an employee might be terminated, these are if the individual has:

a. 'Stolen or smuggled goods and/or money that belong to the enterprise;
b. Given false or falsified information that causes the enterprise to incur losses;
c. Been drunk, consumed intoxicating alcoholic drinks, consumed and or distributed narcotics, psychotropic substances and other addictive substances in the working environment;
d. Committed immorality/indecency or gambled in the working environment;
e. Assaulted, battered, threatened, or intimidated his or her co-workers or the entrepreneur in the working environment.
f. Persuaded his or her co-workers or the entrepreneur to do something that was against laws and regulations.
g. Carelessly or intentionally destroyed or left the property of the entrepreneur exposed to danger, which caused the enterprise to incur

losses;

h. Intentionally or carelessly left his or her co-workers or the entrepreneur exposed to danger;
i. Unveiled or leaked the enterprise's secrets, which is supposed to keep secret unless otherwise required by the State; or
j. Committed other wrongdoings within the working environment, which call for imprisonment for 5 (five) years or more'.[545]

Apart from employees committing the actions stated above, or a change in the status of the company,[546] or employee being absent from work for five days or more consecutively without submitting valid evidence and companies having summoned them in writing,[547] there is no way for companies to dismiss employees, particularly not on grounds of lack of competence or skill:

> 'Entrepreneurs are responsible for improving and or developing their workers' competence through job training'.[548]

Therefore, the ICT companies in this thesis are obligated to improve the skill and competence of their employees through training. The implementation of new technology should not become barriers for employees to keep themselves up. However, one of the interviewees stated that:

> 'However, if they cannot keep up with the development or the changes, they will be fired'. (C4, M)

The ignorance of one of the policy makers of the law could damage the company's reputation in employment. As policy makers, they should be aware of regulation and policy. The company cannot dismiss an employee because they cannot keep up with the development. Moreover, the company should provide employee with sufficient understanding, so they can keep up with the development of technology. There should be some solution for both employees and companies to overcome the changes caused by the implementation of technology. Otherwise, the possibility for employees to commit a crime is likely to happen because they would feel uncomfortable with the situation.

---

[545]Ibid. (n 39), Article 158.
[546]Ibid. (n 39), Article 163-165.
[547]Ibid. (n 39), Article 168.
[548]Ibid. (n 39), Article 12(1).

To be able to keep up with the development of technology, companies need to have a policy related to employees' skill. One of the policies is related to the training on the implementation of technology. However, to stay in the company, the employees themselves should be willing and able to improve their skills in accordance to the company's business strategy.According to one interviewee:

> 'Employees also have responsibility to train themselves, with the new development, if they want to increase their career, they need to learn by themselves. However, if after the training the employee still unable to improve then he's not a competitive person, it will have a negative effect to his career. He cannot get promotion, he will have assumed that he was unwilling to learn, and later he will be included in a group of staff with low performance. He will be given first warning due to his low performance, and then second and third warning. If he performs badly for the three consecutive years, there's no other way than to offer him resignation'. (A1, SM)

Thus, employees themselves have to be willing to learn and improve themselves. The policy maker emphasised that if an employee cannot improve themselves, the company will take action so that they do not become an obstacle for the company to keep up with development. Since the company cannot dismiss an employee for lack of competence, it must offer the employee a golden handshake and silver handshake exit system.

The companies already have exit systems to reduce the number of employees due to the lack of capacity or the age factor. There are two types of retirement, normal retirement and early retirement based on self-request – the exit systems. Early retirement based on self-request is normally caused by the employee committing an offence. However, ICT companies also have another exit system, called the golden handshake and silver handshake. Golden handshake is an executive employee offer with a significant severance package at retirement or termination.[549] Jiang[550] stated that golden handshakes are offered to management that carried high risk in their job. However, this was not confirmed by the policy makers in this thesis. One said that they might have been a good solution for employees and companies to overcome the gap from the implementation of technology and its policy. On those exit systems,

---

[549]Yi Jiang, 'Managerial Incentives in The Presence of Golden Handshakes' (2017) 20 Finance Research Letters.
[550]Ibid.

some compensation was offered to employees if employees would not be able to keep with the company's strategy business. Employees should make a decision whether to improve their skill so they can stay with the company, or participate in the exit programme.

The development of technology has forced companies to speed up the implementation of technology,[551] and that is significant for an ICT company. Employees have to participate and support the company's business strategy by adapting themselves to the current strategy. Policy makers should be able to make a policy that support the company's business strategy.

New policy should not cause a conflict among employees. Policy makers need to make some adaptations so that the new policy will be accepted by all employees. Furthermore, to ICT companies, shifting its strategy to the development of technology is a must. According to one interviewee:

> 'Automatically of course I will follow the development of technology in the future. I see the CSS [CSS] guidance like this, and the development of technology like that. We will make policy that is in line, I will make flexible time, work everywhere, and these are all related to technology'. (A1, SM)

This shows that, to be able to compete in the market, policy makers should be able to make a policy that is in line with the development of technology in the future. This is important, since policy makers realise that the implementation of technology will not only support the development of the companies, but also support all the employees. Companies will prefer to have technology to support them. Policy makers should be able to accommodate the companies' need. If we look at the statement above, the future technology that is applicable in the companies is a technology that supports the flexibility of works. It means that cloud computing will be very valuable in the future.

The interviews have shown that it is necessary for companies, especially for the policy makers to be aware of the aspects related to the protection of personal data kept in their premises, including the personal data of their employees. Data of the employees must be securely kept by ICT companies during the employment cycle, from the

---

[551]Siniša Mitić et al., 'The Impact of Information Technologies on Communication Satisfaction and Organisational Learning in Companies in Serbia' (2017) 76 Computers in Human Behaviour.

recruitment of the new employees until the termination of the employees. We can learn from the approach in EU Regulation 2016/679,[552] that there should be a protection on the personal data of employees, from recruitment to termination.

Another approach that can be learned from is through UK Data Protection Act 2018. UK Act 1998 was upgraded into DPA 2018 by providing how data protection law is being implemented in UK. In DPA 2018, there are provisions that allow an employer to refuse subject access request from employee.[553] Further it is stated that it is prohibited for person to provide another person or giving an access to a record in terms of recruitment, continued employment of a person, and a contract for the provision of service.[554] The implementation of GDPR 2018 encourages the government to give more protection of the personal data, including in the protection of employee.

Undoubtedly, the protection of employees' personal data is clearly stated in the EU Regulation, but this protection does not appearin Indonesian Ministry Regulation 20/2016.[555] The implementation of data security and data protection has given legal certainty for Indonesia's ICT companies to do the business, especially for the cloud industry. However, to make sure that the processing data in the company complies with the regulation and policy, there should be a provision related to the controller or processor or employees who carry out processing of data. The implementation of data protection and data security regulation in ICT companies would influence employees to improve themselves with sufficient knowledge. The legal understanding of ICT employees to comply with the regulations and policies related to data protection and data security would potentially reduce crime during the employment.

Another result from the interviews is that, with the development of technology, policy makers should be able to overcome any difficulty that might arise from the implementation of technology; this could be in technical or non-technical aspects. The implementation of new technology has made a transformation in policy-making.[556]

---

[552]Ibid. (n 26), Article 88(1).
[553]Ibid. (n 278) Part 2, Chapter 2, Art. 10 (1a)
[554]Ibid. (n 278), Part 7, Art 184
[555]Ibid. (n 11).
[556]Ibid. (n 38).

But it is not only policy makers who should be ready for the changes; ICT employees should also be prepared to cope with the development and implementation of cloud computing in the industry, especially to be aware of the impact of cloud security,[557] personal data protection,[558] and the effect of data protection.[559]

4.3 Chapter Summary

The interviews have concluded that the growth of cloud computing has definitely affected business, especially in the ICT industry. The impact is not only for the consumer, but also for ICT companies as a cloud provider. The customer also needs to consider the impact of the implementation of cloud computing. Concerns discussed in this research are on data security, the protection of personal data by the cloud provider, and the roles of data controller and data processor. The interviews show that the implementation of cloud computing has affected employees' behaviour and shifted them into a digital transformation. As a new technology, ICT companies have already implemented cloud computing as a data base. Therefore, ICT employees find no difficulties in the implementation of the cloud for their daily activity. This statement is similar to the finding of Chesley,[560] who stated that the use of technology has an impact on employees, and in their daily lives.

Even though technology has an impact, this does not mean that technology becomes the consideration of policy makers. The reason is because the technology will always change, therefore, policy makers will always consider the business aspect rather than technological aspect, although businesses in ICT will always relate to development of technology. However, policy makers should be aware that in the development and implementation of a new technology, there will always be legal consequences. Therefore, the understanding of the policy makers regarding the implications of the development and implementation of new technology in the companies should be emphasised.

---

[557]Ibid. (n 130), Konstantinos Stylianou, Jamila Venturini and Nicolo Zingales.
[558]Ibid. (n 64).
[559] Antonio Segura-Serrano, 'Cybersecurity: Protection of Critical Information Infrastructures and Operators' Obligations' (2015) 6 European Journal of Law and Technology <http://ejlt.org/article/view/396/592> accessed 5 June 2016.
[560]Ibid. (n 94).

Policy makers will always look at business transformation, which in this thesis is affected by technology. Even though it is important in policy-making, sometimes there is no legal basis related to the transformation. The examples in this thesis are the regulation of ISMS and Protection of Personal Data in the Electronic System which were regulated in 2016, while the cloud itself has already been implemented in ICT companies before the regulations were promulgated. This has shown that the law in Indonesia has relatively lately come to accommodate the development of technology:

> 'Because the law is always one step behind the technology, new technology arrived but the regulation is not available yet, especially in Indonesia … To establish an internal policy, will needs a concept, in the concept, we need to have a clear description and it takes sometimes to do it'. (B2, SM)

This statement, confirmed by all of the policy makers, shows that there is a need for policy makers to have the knowledge and skill to cope the development of technology, in terms of regulations and business purposes. Although the company should be able to apply the newest technology to compete with competitors, policy makers should be aware of the qualification of the product and whether the implementation has any legal consequences or not. Although there is a lack of regulation in technology, it is not a justification for technology not be implemented and marketed. Policy makers should make an approach to government during the implementation period of the regulations to obtain legal protection that can be used to support the business.

The regulations are contained in Law 11/2008 and the Government Regulation 82/2012. Even though it took 4 years to have implementation regulations, Indonesia finally has some protection through regulation of security systems and personal data. Those regulations are important, not only for the customer, but also for the company and its employees. The legal certainty from those regulations guarantees ICT companies in doing their business, especially if it is related to the security systems and personal data protection. The government also promulgated a Presidential Decree establishing the Indonesian Cyber Agency and National Encryption Agency in May 2017 to make sure that government policies related to the cyber security are properly implemented in relation to national security. This agencies need to make sure that they areperforming their tasks. They will involve ICT companies, to make sure that ICT companies also have the supportand protection of cyber security and for the nation.

However, since there is no classification in Indonesian regulations related to the data

controller and data processor, the detailed protection of personal data should be stated clearly in the contract between the cloud provider and the user. It is better for the ICT industry and the government to have clarification of the data controller and data processor roles, to have clear data protection responsibility schemes and to identify who will responsible. As Segura-Serrano[561] stated, it would be better to have a regulatory approach to set an obligation related to the security in the critical infrastructure field. This research agrees with that statement that there should be a specific regulation related to data protection and data maintenance. It is needed for the cloud user to consider the security of their data and how the company will maintain the data in the provider's premises. Therefore, to have a clear understanding of the responsibility, employees of ICT companies should have sufficient understanding of the technology. This is to avoid the intentional and unintentional human mistakes that occasionally happen.[562]

The implementation of new technology in the company is stated in the CSS document. The document will become guidance for policy makers. Since ICT companies put business considerations in making policy, employment policy is also based on the business perspective. Training for improving the skill of employees should support the business perspective. This is similar tothe research finding by Walter[563] that promoting the right training in line with the objectives of the company to improve the knowledge and skill of the employees can reduce maintenance error. Training has been proven to promote the work of employees. Conti[564] stated that training has a positive and significant effect for employees, and Bapna[565] has also stated that training can enhance the performance of employees.

Indonesian regulation[566] has facilitated the employees of companies to have training, however, the policy makers in this research stated that the training should be designed to fit with necessity. This is similar to findings of Barzegar and Farjad[567] that training

---

[561]Ibid. (n 559).
[562]Ibid. (n 115).
[563] Diane Walter, 'Competency-Based On-The-Job Training for Aviation Maintenance and Inspection – A Human Factors Approach' (2000) 26 International Journal of Industrial Ergonomics.
[564] Gabriella Conti, 'Training, Productivity and Wages in Italy' (2005) 12 Labour Economics.
[565]Ibid. (n 35).
[566]Ibid. (n 39), Article 11.
[567]Ibid. (n 15).

should be given to all employees and should be in line with the role of the employees and the organisational needs. However, it is stated in ISO/IEC 27001 that all the employees should have the same understandingof the security system. Therefore the company has to make sure that they provide such training related to the security system. However, this research does not completely agreed with the findings of Hailu[568] that developing countries do not need to have a comprehensive skill in technology. In fact, comprehensive skill is required for the ICT employees to minimise the risk on the implementation of technology in cloud computing.

If we look back at the provision of Indonesian Ministry Regulation 4/2016,[569] it stated that companies should apply the SNI ISO/IEC 27001 standard and safeguard provisions, and ISO/IEC 27001[570] states that employees should be able to protect the information and personal data of the employees themselves or customers' data, it confirms that all the employees in Indonesia's ICT companies should have training related to data security and data protection. The interviews also revealed that policy makers suggest that employees could use the facilities of the companies to address any gaps in skills, and one of the facilities is through online training. This could benefit employees to adjust themselves to the up-to-date technology.

However, the interviews revealed that not all the employees would be willing to accept the shifts caused by the implementation of new technology. Indonesian regulation[571] prohibits the dismissal of employees due to lack of competence. This restriction has made ICT companies find another solution to overcome employees' skill gaps and resistance to the implementation of new technology. One of the solutions is through exit systems, called the golden handshake and silver handshake. The policy makers' effortshere apparently have shown a positive impact on the companies and have been well received by the employees.

This thesis is considering the use of the State-Owned Enterprises (SOEs) Law since the participant in this thesis is an SOE company, therefore, as a parent company, it

---

[568]Alemayehu Hailu, 'Factors Influencing Cloud-Computing Technology Adoption in Developing Countries' (PhD, Capella University 2012).
[569]Ibid. (n 10), Article 7.
[570]Ibid. (n 115).
[571]Ibid. (n 39), Article 150-172.

should be subject to the SOE Law. This regulation should also be obeyed by subsidiaries, since in the making of policy, they have to refer to the parent company's policy.

The first research question looked at to what extent the Indonesian cloud computing industry would be affected by wide-ranging data protection and data security law reforms. From the interviews and regulations in Indonesia, it is clearly seen that the growth of cloud computing has affected the business. By the promulgation of ISMS and Protection of Personal Data in the Electronic System regulations in 2016, Indonesia finally has the legal certainty to do business related to the protection of security system and personal data protection. The ICT business in Indonesia is still growing with the projection of 175 million internet users in 2016.[572] Before the promulgation of those regulations, ICT companies were using ISO/IEC 27001 as international guidance in the security system. However, with the support from policy makers to make an approach to the regulator, the use of ISO/IEC 27001 as guidance is now becoming one of the provisions in the ISMS regulation.

Even though Indonesian regulations have already coped with the development of the cloud computing industry related to data security, there is still a need to highlight data protection, and the roles of data controller and data processor. The need to urge guidance regulation on the data controller and data processor will contribute a huge benefit, not only for the ICT business, but also for the customer as an Indonesian citizen. Although Indonesia has promulgated personal data protection, the clause related to the definition of personal data that should be protected is not clearly stated. To have a comprehensive perception of the type of personal data that should be protected, it is suggested that the government release a statement clarifying the clause to avoid misleading interpretations of personal data in the future. The establishment ofanational organisation supervised by the Ministry of Communication and Information Technology might support data security and data protection. It also gives a legal certainty and educates citizens on the importance of those protections. Legal certainty on the protection of the personal data and the classification of data controller

[572]EU-Indonesian Business Network, 'Indonesian ICT Market' (Your Gateway to Indonesia 2015) <http://www.eibn.org/upload/EIBN_Presentation_ICT_Indonesia.pdf> accessed 23 June 2016.

and data processor will contribute significant factors to the growth of the cloud computing industry in Indonesia.

To answer the second question on the potential impact that data protection and data security law reform could have on the position of employees in the Indonesian cloud computing industry, from the interviews it is clearly seen that employees need to be aware of the newest technology that is implemented and marketed in the company. This understanding can be obtained if policy makers identify and understand aspects in cloud computing. Employees'understanding should also cover the effect of the technology, especially that involves data security, personal data protection, and the roles of data controller and data processor. Policy makers play a significant role in improving the skill of employees. The implementation of cloud computing and the impact of the cloud can contribute a legal aspect to data security, employee's data protection, and clear responsibility of employees as data controller or data processor. Legal certainty on how the company protects and manages the data of their employees and its consumers will bring confidence for the cloud provider in doing their business.

This understanding is not merely related to the technological aspects[573] such as software, hardware, or the system in the cloud, but also related to the legal aspects.[574] Indonesian labour law is adequate in the protection of employees in improving their skills. It is company policy to execute the provisions of the regulation so that the ICT employees have the opportunity to attend training according to their role. However, ISO/IEC 27001, according to Humphreys,[575] stated that: 'The organisation need to ensure that staff are aware of information security risks and have sufficient understanding to support the organisation's information security policy to undertake their normal work functions and tasks. Staff should be trained in the use of information security policies and procedures, security controls applicable to their job function and the correct use of IT (e.g., log in procedures, keeping passwords safe, appropriate use of IT)'. Therefore, since ICT companies are related to information security, the ICT employees should be provided with adequate understanding and skills related to the issues and risk, not only the technological aspects. This means

[573]Ibid. (n 54).
[574]Ibid. (n 54).
[575]Ibid. (n 41).

there is an exception from the Indonesian labour law for ICT companies related to training. However, this exception does not mean that there is a need to reform Indonesian labour law. Moreover, the Indonesian regulations have supported the companies to avoid dismissal.[576] This means that companies need to look for solutions to help some employees who cannot follow or are reluctant over the implementation of technology. One of the solutions from the policy makers is through an exit programme. This programme in ICT companies is relatively successful and it is not against the manpower regulations.

Since the development and implementation of technology in ICT companies is a must and it cannot be avoided and is also in line with the company' strategic plan, policy makers and employees should provide themselves with sufficient understanding and knowledge of the technology. EU Directive 97/66/EC[577] states that companies in the telecommunication sectors should take appropriate technical and organisational measures to provide for the security of their services in relation to the processing of personal data by ICT companies[578] and according to ISO/IEC 27001, which is now mandated by the Indonesian Regulation to be implemented as the security protection in the company, ICT companies need to take steps to prepare their employees in relation to security systems and personal data protection. The Indonesian Regulation should also consider the protection of employees' personal data, from recruitment to termination because there are over 121 million employees in Indonesia.[579]

Policy makers should also assure that employees have an understanding of their important role as data controllers or data processors, since there is no distinction in the Regulation.

---

[576]Ibid. (n 39), Article 151(1).
[577]Ibid. (n 253), Article 4(1).
[578]Ibid. (n 253), Article 1(1).
[579]'Population 15 Years of Age and over Who Worked during the Previous Week by Main Employment Status and Main Industry, 2008 - 2017' (*Bps.go.id*, 2017) <https://www.bps.go.id/statictable/2016/04/05/1911/penduduk-berumur-15-tahun-ke-atas-yang-bekerja-selama-seminggu-yang-lalu-menurut-status-pekerjaan-utama-dan-lapangan-pekerjaan-2008---2017.html> accessed 21 December 2017.

Chapter 5. Recommendations

5.1 Introduction

The aim of this chapter is to present the recommendations of the research, which has sought to analyse the extent to which the Indonesian cloud computing industry would be affected by wide-ranging data protection and data security law reform, and to evaluate the potential impact that reform could have on employees. These recommendations will highlight the improvement in Indonesian data security, data protection, data controller and data processor in aspects of technology and human resources related to the acquisition of skills.

The important issues on choosing those legal aspects of the technologies in cloud computing for the research was based on numbers of cases that has risen recently related to the data security and personal data protection, and how Indonesian government responded the implementation of cloud computing, especially in data security and data protection through enactment of regulations.

These recommendations are in the light of the GDPR provisions and practices as the background of this research as stated in Chapter 1 and Chapter 2 that GDPR is considered as world leading best practice in personal data protection, and also because of business and partnership of EU and Indonesia as well as European Economic Area (EEA) and Indonesia which required an equal data processing, therefore, Indonesia cloud computing companies are obliged to comply with the GDPR.

5.2 Recommendations on Data Security

Subashini[580] stated that every element in the cloud system should be analysed to attract potential consumers. Therefore, Indonesia ICT providers should make sure that their networks, servers, storage, and applications provide for the needs of the consumers. ICT providers should also have to make sure that those services have security protection to prevent any harm that could be caused by failure of the system or unauthorised access to the data.

---

[580]Ibid. (n 157).

From the research findings in Chapter 4, it can be concluded that most of the interviewees agreed that cloud computing is not a new technology. Most of the interviewees interpreted it as storage for data. This is similar to the perspective held by Zhang,[581] that cloud computing is a use of existing technologies to create a new business model by adapting certain technologies to meet the economic requirements of the ICT business. Even though cloud computing is not new for ICT companies, they need to make sure that they comply with regulatory requirement. Therefore, they must make sure that they carry out proper preparation, including compliance with legal requirements, before implementing cloud computing as their business model. This section will present recommendations related to data security as the legal aspect in cloud computing.

Robinson[582] defined security as the confidentiality and availability of data or information, including encryption and privacy as an expression through legal and non-legal norms to protect the right of personal or private life.

It should be borne in mind that the interviews in this research were completed in October 2015. At that time, Indonesia was still looking forward to the promulgation of the data security and personal data protection regulations from the Ministry of Communication and Information Technology. Therefore, to provide protection on the security system and personal data, ICT companies in Indonesia referred to ISO/IEC 27001 until the 2016 regulations were published.

In April 2016, Indonesia promulgated Ministry Regulation 4/2016 which covered how companies, through risk management, were responsible to the public for the performance of electronic systems by giving adequate protection to confidentiality, integrity and availability of information. Interestingly, the Ministry Regulation stated that company should refer to ISO/IEC 27001 on information security. Therefore, being able to relate internal company policy with Ministry Regulation 4/2016 should not be an obstacle, since ICT companies were already aware of the implementation of ISO/IEC 27001 required by the regulation.

---

[581] Ibid. (n 155).
[582] Ibid. (n 216).

The interview findings revealed that, although the regulation was not promulgated until April 2016, all ICT companiesin this research had implemented data security management through ISO/IEC 27001. The rapid development of technology and the later adjustment of the regulation did not delay ICT companies in extending their businesses to meet customer requirements. Policy makers stated that they had made an approach to the government to cope with the lack of regulation to make sure that the business is in line with the draft regulation. Meanwhile, to cope with the lack of regulation, policy makers specified the agreement between each party in a contract, even though the contract is merely basic contract law.

Policy makers stated that there are some unclear regulations in Indonesia, which might lead to misperception that would delay the ICT businesses. Therefore, the following sections detail some recommendations in the field of data security. These recommendations will put forward legal reforms to clarify the law in Indonesia, with the aim of making regulation in data security more precise. This will prove beneficial to both employer, when developing policies, and employee, in providing a more robust framework leading to accurate application of the relevant law.

5.2.1 Standard guidance on security system compliance

The findings in Chapter 4 reveal that one of the interviewees (B2, SM) stated that the company has its own certification for the security system, called ISO. This is similar to the provision on the Indonesian Ministry Regulation 4/2016[583] that emphasised the protection of security systems, ICT providers should refer to ISO/IEC 27001 as international guidance in ISMS. It is therefore crucial for ICT providers to make sure that they comply with the provisions of Ministry Regulation 4/2016 and ISO/IEC 27001. To comply with the regulation and ISO guidance, the company should have a standard risk management system in the company that consists of monitoring, auditing and reviewing the security system, and it should be updated regularly. The standard of the security system should be in the company policy and comply with by employees. To make sure that employees understand the updated security system, they need to read and sign an integrity pact to make sure that they are up-to-date with the current

[583]Ibid. (n 10), Article 7.

security management system and know that they are responsible for the protection of confidentiality data in the company. The integrity pact is sign annually and the announcement is appearing in the internal company portal and it is emailed to all the employees.

However, aside from that, employers have a responsibility to offer a specific training in accordance to the business requirement in the company and employers are not required to make attendance at/ completion of training compulsory, unless the employers also taking part in the training.

5.2.2 Implication of ISO/IEC 27001 as guidance in the Indonesian Regulation

Ministry Regulation 4/2016 regarding ISMS has brought legal certainty for electronic operators in Indonesia, particularly in managing security systems and protecting personal data. For the ICT companies in this research, it is a privilege for them to have applied ISO/IEC 27001 as guidance in their security system, which is emphasised by the Regulation. The promulgation of Ministry Regulation 4/2016 will give confidence and legal certainty to ICT companies when expanding their business. However, since the government has set out guidance on security system under ISO/IEC 27001,[584] if there is a new guidance on the security system, there should be continuous adjustment to the guidance. It is important to investigate whether to give ISO/IEC 27001 as a guidance in the regulation will be enough to cope with the future development of technology. If ISO/IEC 27001 isrevised with some additional guidance on the security system, the Indonesian Regulation will need to be amended, and to make an amendment will take some time. This can be seen in the promulgation of Ministry Regulation 4/2016 that took almost four years from the provision of Government Regulation 82/2012[585] on electronic system andtransaction operation. This will raise another uncertainty for businesses to keep upgrading security systems to increase the performance of the business while the Regulation still refers to the pre-update security system.

[584]Ibid. (n 10), Article 7.
[585]Ibid. (n 253), Article 14.

5.2.3 Review of the promulgation of the Indonesian Regulation

It took four years to promulgate Ministry Regulation 4/2016 to update Law 11/2008 and Government Regulation 82/2012. The aim of Ministry Regulation 4/2016 was to give legal certainty on security systems, especially in the relation to protecting personal data. The Regulation referred to ISO/IEC 27001 as guidance as it is the latest up-to-date international security system when the Ministry regulation promulgated. However, ISO/IEC 27001 itself has made several improvements to cope with the development of technology.

ICT Companies has also had to make sure that they have the up-to-date security systems for the protection of personal data in their promises. These up-to-date security systems need to cover the protection for the data of the employees in the company, the company itself, and personal and sensitive data of the customer. The protections should be able to cope with the high changeability of the development of technology. Therefore, there should be a protection regulation that covers the aspect of security in general. Referring to specific guidance will make the regulation inflexible to the development of technology. Technology will always change rapidly, and regulation should be able to support the development of technology and the business.

The rigid and specific regulation will slow the business in providing itself with up-to-date technology. The influence of the regulator and other obstacles like the economic or political environment in Indonesia might be another reason for delaying the regulation. Future research should investigate whether the economic or political environment or other obstacles might cause delay in theIndonesian government promulgating regulation on data security. Policy maker B3, SM suggested that there should be synchronisation between business and economic aspects, information and technological aspects, and the law, to establish a comprehensive regulation in Indonesia. Therefore, investigating potential delays might help the Indonesian government to cope with the high-level aspects in the development of technology in Indonesia.

5.3 Recommendations on Data Protection

Jakimoski[586] stated that cloud providers should make sure that they protect the data of their consumers. To make sure that a company covers all categories of personal data protection, there should be clear conception of the personal data. The UK's Data Protection Act 1998 defines categories of personal data, and EU Directive 95/46/EC[587] describes how to identify personal data that should be protected. EU Regulation 2016/679[588] requires that dealing with personal data means it should also include sensitive data as defined in the DPA. Personal data, according to EU Regulation 2016/679,[589] is any information that can identified a person directly or indirectly, by using an identifier such as name, identification number, location data, online identifier, medical, economic, culture or social identification.According to DPA,[590] sensitive personal data refers to racial or ethnic origin of the data subject, political opinion, religious beliefs, membership of a union, physical or mental condition, sex life, the commission or alleged commission of any offence, and any proceedings for any committed offence. This mean the EU has broadened the protection of personal data by adding sensitive personal data to data that should be protected, and this is stated in the regulation.

Indonesian Ministry Regulation 20/2016[591] has not explained the categories that could be included on personal data. Despite giving a clear explanation of the personal data, the Regulation states that there would be further explanation regarding personal data and its implementation. The interview findings revealed that policy makers in ICT companies have made policy related to the data that is kept on the premises. Even though ICT companies have delivered the infrastructure to the cloud provider, ICT companies as the customer have control to manage the authority, password and access to the data. Although policy makers assumed that cloud computing was accessible for data sharing in the company, it should be understood that it might contain sensitive personal data that should not be shared without some restrictions. To classify which

---

[586]Ibid. (n 475).
[587]Ibid. (n 25).
[588]Ibid. (n 26).
[589]Ibid. (n 26), Article 4(1).
[590]Ibid. (n 278), Chapter 29, Part I (2).
[591]Ibid. (n 11).

data might contain a specific personal data, there should be a provision in the regulation and company policy that standardises terms of personal data. The recommendations related to data protection are below.

5.3.1 Criteria of personal data

The effect of Ministry Regulation 20/2016 is that ESOs should treat the personal data that is managed by them carefully. Even though it was stated clearly in the Regulation how ESOs should tread their customers' personal data, it was not explained what categories of data should be protected. It also does not mention that the process can be delegated to an electronic agent as a third party, as stated on the Government Regulation 82/2012.[592] Therefore, to give a legal certainty to data owner and the ICT company as ESO, it is advisable to create a legal regime that puts a responsibility on organisations to state clearly on the contract between the user and provider the criteria of personal data that should be protected by the provider. In a contract clause, it would be clearer if the provider stated that provider will protect the personal data of the user which include to the information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who 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.[593] However, if the specific criteria of personal data are stated in the regulation, then it would not be necessary for provider and user to state it on the contract.

5.3.2 Definitions of personal data and sensitive personal data

The Ministry Regulation 20/2016[594] has brought a new paradigm on how personal data should be protected by the ESO, but without clearly stating the category of personal data that should be protected. Article 34 states that there will be a consultation session for public related to personal data protection and its implementation, but there should be a comprehensive clause in the regulation related

---

[592]Ibid. (n 253), Elucidation.
[593]Ibid. (n 26) Chapter 1 Article 4(1)
[594]Ibid. (n 11).

to the personal data specification. Providing clear definitions of personal data and sensitive personal data in the regulation, which is similar in approach to the EU Regulation[595] and the DPA,[596] will avoid the differences in interpretation.

The government could establish a specific group to manage and control the implementation of the protection of personal data, similar to the WP[597] and DPO in the EU.[598] This is important, since law enforcement on data protection is relatively new in Indonesia but there is no further explanation of the categories of personal data that should be protected by the law, and the public need to have a same perception on the important of data protection.

5.3.3 Reforming Indonesian personal data regulation by stating the definition of personal data in the regulation and employees' personal data protection

The DPA, EU Directive 95/46/EC and EU Regulation 2016/679, have clearly stated the category of personal data protection that should be protected, but the Indonesian Regulation does not. It is important to have a same perception related to the categories of the personal data and sensitive personal data, to avoid misconception on the terms.

Another suggestion related to the protection of personal data is to have a provision on the regulation related to the protection of employees' personal data. The EU Regulation,[599] gives an example of how important it is to protect personal data. However, this protection has not been discussed in the Indonesian Regulation. It is necessary for the Indonesian government to start to think of the protection of personal data in the relation of employment, since there is huge number of employees in Indonesia.

Further research is also suggested for reviewing the protection of personal data and sensitive personal data for in-house IT systems in other sectors, such as the economic sector, public services, defence or national security, and in law enforcement

---

[595]Ibid. (n 26), Article 4(1).
[596]Ibid. (n 278), Chapter 29, Part I (2).
[597]Ibid. (n 494).
[598]Ibid. (n 26), Article 37-39.
[599]Ibid. (n 26), Article 88(1).

institutions such as the police or prosecutors. These reviews are needed since those sectors directly deal with personal data. There will be personal data that should be protected, such as bank accounts, personal identities, health data, location data, or any online identifier as stated in Article 4(1) of EU Regulation 2016/679.

5.4 Recommendations for Data Controllers and Data Processors

One of the benefits of deploying cloud computing as a business model is that the company does not need to have its own technology infrastructure. It can outsource the infrastructure according to its needs, including service and maintenance.[600] However, the cloud provider should guarantee to provide and update the data security protection on the system, and protect the user's personal data. Therefore, the cloud provider should make sure to provide its own employees with the adequate competence, skill, and knowledge to understand their responsibility in the cloud business.[601] Employees should be able to identify their work tasks and be responsible for the authority that they have.

The DPA,[602] EU Directive 2016/680[603] and EU Regulation 2016/679[604] elaborate on the classification of organisations with a responsibility for processing of personal data. However, there is no classification of such organisations in Indonesia. The interview findings show that ICT companies as a cloud provider play a role as an integrator. This means that the company might deliver the obligation itself, or it may delegate the obligation to another party, this means to the electronic agent. There is no compulsion onthe cloud providers to determine themselves as a data controller or data processor as in the EU regulation. Therefore, the recommendations related to data controller and data processor are below:

5.4.1 Delegating responsibility on the contract between parties

The impact of Indonesian Regulation on delegating responsibility from ESOs to electronic agents would bring a legal uncertainty to the protection of personal data.

---

[600]Ibid. (n 157).
[601]Ibid. (n 74).
[602]Ibid. (n 25), Section 1 (1).
[603]Ibid. (n 27), Article 3 (8,9).
[604]Ibid. (n 26), Article 4 (7).

This situation might arise if it has not stated clearly on the contract between customer and the ESOs that ESOs will delegate its obligation and responsibility arise from the obligation to an electronic agent.

Therefore, it is advisable to create a legal regime that puts a responsibility on organisations to state clearly on the contract between the user and provider the obligation and responsibility of ESOs to manage the personal data in their premises. In a contract clause, it would be clearer if the provider stated the obligation and responsibility of provider and user as stated in GDPR in the regards of data controller and data processor. This is important for the cloud computing industry, since in the business, ICT companies might act as the ESO or as an electronic agent, or might deliver the data to a third party without any consent from the data subject.

If we look at EU Regulation 2016/679, consent means:

> 'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[605]

Therefore, any change in the processing of personal data should be stated clearly, including which organisation will be responsible for the data.

5.4.2 Reforming the classification of specific organisations on processing personal data in Indonesia

Indonesian regulations do not recognise the separation of responsibility of organisations as mandated in the EU. However, under Article 35 of Government Regulation 82/2012, electronic agents might have similar responsibilitiesas data processors which work on behalf of the ESO.An electronic agent, according to Government Regulation 82/2012[606] is a device of an electronic system to perform an electronic transaction. Government Regulation 82/2012[607] also states that ESOs could delegate electronic transactions to electronic agents, and Indonesian Law 11/2008[608]

[605]Ibid. (n 26).
[606]Ibid. (n 253), Article 1(3).
[607]Ibid. (n 253), Elucidation.
[608]Ibid. (n 319), Article 21(2c).

states that if the electronic transaction is conducted through an electronic agent, all the transactions will become the responsibility of the electronic agent.

Even though Indonesian regulations state that ESOs might delegate their obligation to electronic agents, it should be clear on the process of delegation. It should also be stated on the contract between customer and ESOs related to the process and who will be responsible for the data security process and the protection of personal data. This also need to be state on the contract the clearer responsibility on who will perform as the data processor as well as who will act as data controller as stated in GDPR. If the new data protection regulation in Indonesia has stated clearly about this distribution, then it won't be necessary to state it again on the contract. However, since Indonesia regulation has not state it clearly, this contractual provisions might act as a substitutes of the lack of clauses in Indonesian regulation. The statement is required since Indonesian regulations do not regulate a separation of responsibility between data controller and data processor as in EU Regulation. This clear separation will support ESOs and electronic agents to deliver their obligation and give legal certainty for customers related to their personal data protection.

Therefore, there is a need to reform Indonesia's data protection laws to state clearly who will be responsible for personal data protection by stating in the regulation a clear responsibility of for ESOs and electronic agents, and whether delegating the electronic transaction will eliminate the responsibility of the ESO. The Indonesian regulator might refer to the approaches in EU regulations by splitting the roles of data controller and data processor. This is because ESOs and electronic agents have a similar role and obligation as the data controller and data processor, but not to the responsibility for personal data in electronic transactions if the obligation was delegated to an electronic agent. Therefore, the clause in Government Regulation 82/2012 related to the delegating of electronic transactions needs to be re-examined and there should be a government control related to the delegating process from provider to a third party.

5.4.3 Re-examining the provision in Indonesian regulations related to the responsibility ofESOs and electronic agents

The provisions of Government Regulation 82/2012 related to ESOs and electronic agents do not have the same legal force as those for data controller and data processor in the EU Regulation. The obligation and responsibility of data controllers and data

processors is stated clearly in the EU Regulation,[609] while Indonesian Ministry Regulation 20/2016[610] states the responsibility of the ESOs and Government Regulation 82/2012[611] stated the responsibility of electronic agent as a behalf of ESO.

Indonesian Law 11/2008[612] states that ESOs are no longer responsible for the protection of personal data when electronic transaction are delegated to electronic agents. Therefore, there is no legal requirement for ESOs to be responsible for personal data if electronic transactionsare delegated to electronic agents. The responsibility will be borne by the electronic agent alone. Since there is no clear separation of data controller and data processor in Indonesian Law, it is suggested to re-examining the provision on Indonesian Law 11/2008, Government Regulation 82/2012, and Ministry Regulation 20/2016, related to the responsibility of ESOs and electronic agent in protecting personal data. This is to make sure that in processing personal data, ESOs and/ or electronic agent have fulfilled the data protection principles.

However, in the EU Regulation,[613] when a processor delegates another processor to carry out the processing activities, they still have the responsibility to perform personal data protection. The delegation does not wave the processor's responsibility. It also states that, without any instruction from the data controller, the data processor shall not process any personal data.[614] Referring to the EU Regulation,[615] the data controller and the data processor have to make sure and demonstrate that they perform appropriate technical and organisational measurements related to personal data protection. It clearly states the distinction between the two and each organisation cannot exceed the authority of the other. This clear classification will simplify the tasks and responsibility of each. Therefore, it is important for the Indonesian government to make a clear provision in the regulationsas to which organisation will bear the responsibility of protecting the personal data, to give a legal certainty to

[609]Ibid. (n 26), Chapter Four.
[610]Ibid. (n 11), Article 28.
[611]Ibid. (n 253), Article 35.
[612]Ibid. (n 319), Article 21(2c).
[613]Ibid. (n 26), Article 28(4).
[614]Ibid. (n 26), Article 29.
[615]Ibid. (n 26), Chapter Four.

customer, ESO and electronic agent.

5.5 Recommendations for Human Resources

An up-to-date understanding of the issues and risks in the information security and technology and business practices[616] would ensure that cloud technology is properly supported, regulated and protected in the business. Even though, according to the interviewees,cloud computing is not a new technology in ICT companies, changes are still needed in employees' skills.[617] They also stated that cloud computing has changed the behaviour of employees.[618] In particular it has resulted in building awareness of the importance of data security and data protection,[619] and has built an ecosystem between units in the company based on technology.[620]

Other findings from the interviews show that there is a need for the ICT employees to adjust to the development and implementation of new technology. The ICT companies have already provided them with some support, but this is limited and needs a more coherent strategic plan, and to be properly funded, such as face-to-face training, online training, or other educational programme, but these need to be closer together and consolidated. Because of budget problems, policy makers will consider an approval for training related to the companies' strategic plan, which is often related to training intended for technical competence. However, the provisions on ISO/IEC 27001 state that all the employees in the field of security systems need to keep up-to-date with the issues and risk in the information security. Therefore, all ICT employees should update themselves on the security system; however, this becomes difficult if ICT companies are hiding behind budgets and strategic plans. If we learn from the approach under EU Regulation 2016/679,[621] which states that the protection of personal data should be understood by all employees, this means that companies should make sure that all of their employees are aware of the requirements of data security and personal data protection.

---

[616]Ibid. (n 41).
[617]Ibid. (n 1).
[618] As stated by A1, SM.
[619] As stated by B2, SM.
[620] As stated by C3, SM.
[621]Ibid. (n 26), Article 88(1).

This understanding of the security system should be reflected in the life cycle of employment. According to the interviews and the CSS, to keep up with the development of technology and also stated on the, policy makers are tending to recruit digitally literate employees as a recruitment policy. The implication of this method is that employees in the companies are challenged to update themselves with technology to avoid any gap that might arise between the new employee and the existing employees.

It was also revealed in the interviews that current employees should also be updated. However, in the implementation of technology, there are some obstacles that might be faced by the company, such as the age gap,[622] education gap,[623] or lack of knowledge.[624] Policy makers must think of a way to overcome this problem. If there is new technology that requires an expert, ICT companies have a tendency to recruit experienced professionals for a short-term need, rather than to recruit fresh graduates with minimum experience. However, this short-term solution has created some problems, such as they might be rejected by existing employees, since they occupy a job position that employees think should be for them. Another problem is that the salary of the professional expert is usually higher than that of an existing employee, so it would make a huge gap between existing employees and the professional expert.

To maintain the integrity of employees in the company, they should sign the integrity pact annually, which encompasses integrity, business ethics, and data confidentiality. This shows the company has a preventive programme to support the security system and personal data protection. The recommendations related to human resources aspect are listed below.

5.5.1 Continuous learning and the security system

Indonesia, with the huge potential internet market, should be supporting the knowledge and skills of the employees of ICT providers related to the aspects of the technology. Some 65% of Indonesians are connected to the internet, and this percentage will rise further.

---

[622]Ibid. (n 97).
[623]Ibid. (n 98).
[624]Ibid. (n 99).

Despite cloud computing technology being familiar in the ICT business, there are several considerations regarding its implementation. Referring to ISO/IEC 27001, employees, including management, should comply with the regulation by referring to the ISMS in doing business. This includes the policy-making process. Therefore, as part of PDR, employees should identify their skills and training, which could then be assessed against the regulations on data security and data protection. This would then form the basis for identifying further training needs.

Technology in the office might be misused by employees.[625] This can be through sharing passwords and sensitive information,[626] software piracy,[627] and using internet access for their personal purposes.[628] This potential crime in the office should be prevented through a security system, including the integrity pact which increases employee understanding and can update changes in policy to prevent breaches.

The approach on the EU Directive 97/66/EC[629] states that companies in the telecommunications sectors should take appropriate technical and organisational steps to provide the security of their services in relation to the processing of personal data.[630] Therefore it is best for ICT companies in Indonesia to make sure that all of their employees are aware of and implement all of the compliance related to the security system and personal data protection.

It is also suggested that the policy makers ensure that there is a continuous learning process on the understanding of policy regarding the security system, including its process and development, to build the skill and knowledge of the employees. The learning process could be achieved through leadership training and competence training.[631] Since budget and approval from the supervisor[632] has become an obstacle to a training, the company might have training through e-leaning that is accessible anytime and anywhere for all employees. However, companieshave to make sure that

[625]Ibid. (n 286).
[626]Ibid. (n 289).
[627]Ibid. (n 287).
[628]Ibid. (n 288).
[629]Ibid. (n 253), Article 4(1).
[630]Ibid. (n 253), Article 1(1).
[631] As stated by A1, SM.
[632] As stated by A2, SM.

the training modules are updated with the developments of technology, business, and law.

5.5.2 Employees' perspectives

This research looked only at policy makers. Future research might seek to gain an insight from ICT employees on how the implementation of policy has affected their behaviour to find out the effectiveness of the policy on the development of employees' skill. It will reveal if policy in the company has supported employees' development from their perspective and enrich the findings on how policy makers have included the regulation aspect, business aspectand the employees' insight in policy-making related to the development of skill in the company.

The insight from employees might give a perspective to the policy makers on the extent to which the company supports improving the skill and understanding of the employees related to the implementation of new technology. It could also reveal the obstacles facing employees due to the implementation of new technology and give feedback to the policy makerson the implemented policy.

5.5.3 Directors' perspectives

This thesis has revealed the importance of the understanding of legal aspects in the implementation of new technology of cloud computing. The insights from the policy makers have also revealed that the implementation of new technology as stated in the CSS has brought some changes in policy-making. This statement is in line with the findings of Janssen and Helbig[633] that the aspects of policy-making change due to new technology. However, in policy-making, policy makers are required to align the company's ratified strategy with the employees'need to achieve the strategy and the approval from the relevant director.

Further research could review the extent of director approval related to policy-making to support the development of employees' skills, to determine whether the director has given approval and agreement to the policy made by the policy makers. This will also look at what the consequences would be if the director rejected or disapproved the

[633]Ibid. (n 38).

policy. Approval is important to support the execution and the implementation of the policy and to make sure that the policy gives appropriate protection to the employees.

5.6 Chapter Summary

This chapter highlights that, to have a comprehensive understanding of the legal aspects of cloud computing, there are further steps needed. The Indonesian government supports the protection on data security and personal data as promulgated by Ministry Regulation in April 2016, including protection of data security and personal data protection, but some issues remain outstanding. This chapter makes recommendations to complement the existing regulations on data security and personal data protection.

Zhang[634] argued that cloud computing is an expansion of the existing technology that creates a new business model to meet the economic requirements for ICT business, but this raises some legal issues concerning data security, personal data protection, and data controllers and data processors.

The Indonesian Ministry Regulation promulgated in April 2016 emphasised the use of ISO/IEC 27001 as guidance for security systems,[635] but even with that there is a need to ensure employee awareness through the integrity pact. The approach to the government on data security has indirectly generated the use of ISO/IEC 27001 in the Regulation. Although this might benefit the companies, it might have consequences if there is an updated security system. Stating a rigid and specific regulation as a provision might delay the implementation of new security system, which might lead to damage to the business. Therefore, it is suggested to review the provision on the use of ISO/IEC 27001 on the regulation to cope with the rapid development of technology.

This chapter also highlighted the criteria of personal data in the Regulation. Unlike the UK and EU regulations that clearly state the definition criteria of personal data and sensitive personal data that should be protected, the Indonesian regulation does not mention clear criteria. To have legal certainty on data protection, there should be a

[634]Ibid. (n 155).
[635]Ibid. (n 10), Article 7.

clear definition. This might be done in the contract between parties related to the personal data that should be protected by the ESO. Adding the definitions to the Regulation would also avoid different interpretations being used. It is also suggested to have insight from other sectors, such as economic sectors, public services, defence, national security, the police and prosecutors. This is because those industries also deal with personal data, which falls under the definition in Article 4(1) of EU Regulation 2016/679.

Another suggestion is to give more protection to employees' personal data. Indonesia, with a large workforce, should consider giving more attention to the protection of personal data. The EU and its member states have already put some consideration into giving more protection to employees, however, this provision has not been included in the Indonesian Regulation. It is important that employees have legal certainty related to their personal data and how the companies control and process it during the employment cycle.

Recommendations related to data controllers and data processors emphasised the importance of having a separation of responsibility in the organisation dealing with personal data protection. This recommendation also highlighted the terms of ESOs and electronic agents in the Regulation which allows ESOs to delegate their tasks and responsibilities to electronic agents. However, the regulation does not explain to what extent the task and responsibility might be delegated. To give legal certainty in the business, it is suggested that the Indonesian government should make a clear provision related to the classification of organisations that will bear the responsibility of protecting the personal data.

Referring to the Tasks of the EU's WP,[636] which was the EDPB under EU's General Data Protection Regulation,[637] the Indonesian government might establish a national organisation supervised by the Ministry of Communication and Information Technology to ensure that ESOs and electronic agents have a sufficient security system and protect customers' personal data. This will lead to the enforceability of right that would happen if there is a strong of regulation to overcome the breach of the

[636]Ibid. (n 494).
[637]Ibid. (n 26), Article 68.

contract.

A strong regulation in personal data protection and data security would minimize the data breach in the premises. Law enforcement through national supervisory and enforcement powers should also be stated on the regulation. The implementation of regulation on personal data protection and data security should also be spread among people in Indonesia, and regulator had to make sure that Indonesian citizen had already aware and understand the right and responsibilities in personal data protection and data security. A supervisory and enforcement powers model as offered in GDPR might be a good example for Indonesia regulation and the national regulator to take enforcement action against data controller and data processor in the absence of a complaint by an individual data subject.

Therefore, ICT companies in Indonesia should have a statutory obligation to comply with data protection and security laws, and failure to do so could lead to breach the law which national regulator could enforce (as opposed to an individual complaint, contractual model).

National regulator as offered in GDPR, has the power to monitor, advisory, issuing guidelines, recommendation, and best practice, examine, reviewing, carry out the accreditation of certification bodies and maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism in the relation of data protection, as well as to make them public. They might also consult interested parties and give them the opportunity to comment within a reasonable period.

Indonesian national regulator should have the same power to develop guidance similar as EDPB in GDPR, which regarded as expert and authoritative by Courts. This body will act as representative of government on behalf of data subjects and industry. The establishment of the national organisation will be to make sure that ICT companies fulfil the provisions related to data protection principles and advise on the security of personal data. The body should make an annual report regarding the protection of personal data which include a review of the guidelines, recommendations and best practices and shall be made public.

As it is supervised by Minister of Ministry of Communication and Information Technology, this body is has the role to oversee and make sure that regulation in

personal data protection is well implemented and applied constantly in Indonesia, and also to make sure the effective cooperation amongst Minister of Ministry of Communication and Information Technology and ICT industry.

The understanding of the technology not only relates to technical aspects, but also to legal aspects. The recommendation on Human Resource aspects reveals that policy makers should ensure that their employees comply with the regulations on data security and personal data protection. This could be done through the annual signing of an integrity pact, ensuring that the company has adopted the latest security system and employees are aware of the up-to-date security system. The provision in ISO/IEC 27001 and EU Directive 97/66/EC emphasise that it is a requirement for the ICT employees to understand and keep updated with issues and risk in the information security to support the development of the technology itself and business practices.

A continuous learning process on the understanding of the security system, including its processes and development, is also necessary to build the skill and knowledge of the employees. This research also makes recommendations on the effectiveness of the policy in the development of employees' skill, to enrich the findings on employees' insight in the policy-making and the relevant directors' approval of the policy on the development of skill in the company.

In general, the Indonesian government has supported the development of technology through the promulgation of Ministry Regulations 4/2016 and 20/2016. However, there are still some recommendations to support those regulations to be more comprehensive and have strong legal enforcement. Flexible provision related to the security system is intended for ICT companies to adjust their security system of the latest up-to-date system. Clear and common perception of the definition of personal data will avoid different interpretations related to the classification of the personal data that should be protected. The establishment of a national organisation, which might have a similar task as the EU's EDPB, which is to monitor and make sure that the regulation has been properly implemented, giving advice related to the protection of personal data, data controllers and data processor, and giving guidelines, recommendations and best practice related on how to maintain the data in accordance with Indonesian regulation. A continuous learning process related to technological and legal aspects and insights from employees might contribute to the policy makers'

perspective in policy-making.

Chapter 6. Conclusion

6.1 Introduction

This research has explored how data security, personal data protection, data controllers and data processors in cloud computing have affected the policy makers in ICT companies in making their policy, and has probed how Indonesia's laws should develop. It has also revealed the policy makers' understanding of cloud computing, how they make policy in the company, how they support the development of employees' skills, and what solutions they have to overcome problems related to the implementation of cloud computing. Legal aspects in this research focused on data security, personal data, and data controller and data processor in the relation to the ICT companies' employees.

This research is fresh, as the relevant regulation was only promulgated in 2016. It focuses on the implementation of data security and personal data in ICT companies in Indonesia as the researcher had access to the companies due to being an employee of one of them, and the companies themselves supported the project. Therefore, the results of the interviews of this thesis are original and unique because the researcher is researching phenomena occurring in her own workplace.

With the publishing of two significant regulations in ICT in 2016,[638] the Indonesian governmentis already aware of the importance of data security and the protection of personal data, which is important in the development of technology in Indonesia. It has also been stated that there will be further guidance for security system and personal data in the form of further Ministerial Regulations.

There are still some considerations to make those regulations more comprehensive. Chapter 5 stated that there should be standard guidance on security system compliance for ICT companies. It also concernsciting ISO/IEC 27001 as guidance in the regulations, since stating a specific security guidance might have an effect on implementing new security guidance in technology. Section 5.3 argued that there should be a similar perception on personal data and the criteria of personal data to

[638]Ibid. (n 10); Ibid. (n 11).

make sure that ICT companies and the government provide adequate protection for citizens' personal data. Section 5.4 stated that it is important to have a national organisation to make sure that ESOs and electronic agents have a sufficient security system to protect customers' personal data, and section 5.5 recommended having a continuous learning process on the understanding of security policy in the company.

This thesis has used empirical legal research through insights from policy makers in Indonesia's state-owned ICT companies and in analysing regulations and policies in the EU, the UK, and Indonesia.

This chapter will highlight whether the research hypothesis is consistent with the research findings in Chapter 4. This chapter will also state the strengths and limitations of the implementation of the research methodology andhighlight the contributions of the research.

6.2 General Conclusions and Discussion

Cloud computing is technology that involves innovation in the industry, the company environment and the service product. Using cloud computing requires the readiness of networks, servers, storage, applications[639] as well as the awareness of people of the important role of the cloud service.[640]

Many issues could affect the implementation of cloud computing, such as the contract clauses,[641] privacy,[642] principles in data protection,[643] network security[644] and data security.[645] This research has highlighted data security, personal data protection, and

---

[639]Ibid. (n 199).
[640]Ibid. (n 212), Nesrine Kaaniche and Maryline Laurent.
Ibid. (n 200), P. Ravi Kumar, P. Herbert Raj and P. Jelciana.
Ibid. (n 212), Duha Alsmadi and Victor Prybutok.
Ibid. (n 199),
Ibid. (n 212), Gregory Levitin, Liudong Xing and Yuanshun Dai.
Ibid. (n 212), Ashish Singh and Kakali Chatterjee.
Ibid. (n 212), Gururaj Ramachandra, Mohsin Iftikhar and Farrukh Aslam Khan.
Ibid. (n 212), Syed Asad Hussain et al.
Ibid. (n 212), Saurabh Singh, Young-Sik Jeong and Jong Hyuk Park.
[641]Ibid. (n 61).
[642]Ibid. (n 53).
[643]Ibid. (n 64).
[644]Ibid. (n 63).
[645]Ibid. (n 54).

data controllers and data processors, which are crucial for ICT companies to have legal certainty in cloud computing in Indonesia. This research was enriching by perspectives from cloud users,[646] cloud providers,[647] and study of the regulations[648] in seeking the consistency of existing regulations with the real situation for ICT companies in Indonesia. The research presented in this thesis was focused on the level of the ICT provider as a user and a provider at once. It examined the policy makers' considerations, such as background and perspective on cloud computing, how cloud computing has been implemented in companies, and how employees cope with the legal aspects of it. The fundamental understanding of cloud computing was highlighted in Chapter 1 and explored in depth in Chapter 2. Those chapters explore the appraisal of cloud computing and data security, data protection, data controllers and data processors as legal aspects of technology, and the human resource aspects related to their skill to cope with the development of technology in the company. These chapters also stated the government position through regulations and policies in each aspect of the technology. Chapter 3 specified the methodology used to examine the relation between company policy, the development of technology, and regulations implemented in the company. Policy makers' perspectives in this research were used to examine the policy-making process in ICT companies and whether Indonesian information law reform could affect the cloud computing industry and the position of employees. Policy makers' perspective become an important input for the research to figure out to what extent employees in ICT companiesare aware of and implement the protection related to data security and personal data protection in the company.

Chapter 4 stated that policy makers as the participants in this research were selected from high-level management in Indonesian ICT companies who have a role in policy-making and influence on the policy in ICT companies. The interesting aspect of this research is that the policy makers interviewed in this research were from a state-owned company and its subsidiaries. The different entities of those companies are subject to different regulations borne by each company; however, this research revealed that apparently the policy made in the subsidiary companies must refer to the

[646]Ibid. (n 56).
[647]Ibid. (n 157).
[648]Ibid. (n 162).

regulations that bind the parent company.

The findings of this research were presented in Chapter 4., where policy makers' perspectives were compared with the existing regulations and policies in the EU, UK, and Indonesia. Although the Indonesian government promulgated regulations after the interviews were conducted, they gave insights into how ICT companies cope with the lack of regulation in such areas of technology. Furthermore, policy makers' perspectives in cloud computing will enrich human resource policy in managing the gaps of skill in Indonesia's cloud industry as a developing country.[649]

The research recommendations and potential aspects for future research stated are in Chapter 5. The findings of the interviews are moulded from the insights of policy makers in ICT companies, who assumed that employees are already aware of cloud computing as it was implemented in the company since the 1990s and used as data sharing amongst employees. Section 5.2 revealed that ICT companies implemented ISO/IEC 27001 before the Indonesian Ministry Regulation was promulgated in April 2016. The approach made by policy makers to government has demonstrated that there is a need for regulation in the ICT business to support the development of technology and the business. Section 5.3 revealed that it is important for the business, customer, and government to have the same perspective related to the classification of sensitive personal data that should be protected by ICT companies. Section 5.3 also emphasised the importance of protecting personal data for employees. There is no provision in the Indonesian regulations which states the protection of personal data in the relation to employment. This is important for the protection of the employees themselves.

Section 5.4 stated that clear delegation between electronic system provider and electronic agent would give legal certainty to the business related to control and processing of personal data of the customer. Section 5.4 also highlighted the establishment of a national organisation to make sure that ESOs and electronic agents have provided a sufficient security system and protected personal data.

Section 5.5 stated that the ecosystem related to development of technology will

---

[649]Ibid. (n 568).

support employees to enhance their skill. Technical training and expert recruitment might become a fast solution to cope with the skills gap; however, employees should be able to give themselves sufficient skill in the development of technology. Employees need to make sure that they are aware of up-to-date technology as the business core of ICT companies, and they have to comply with the policy and regulation related to the business.

Research literature reviewed in Chapter 2 stated that a number of researchers have tried to define cloud computing,[650] however, the interpretation from Zhang[651] stated that cloud computing is existing technologies gathered into a new operational business model and this has the most similar approach tothat revealed by the policy makers' interviews in Section 4.3. The main research aim of this section was to explore the understanding of cloud computing implementation in the company by policy makers. The interviews revealed that most policy makers are aware of the definition of cloud computing as data storage and they have implemented cloud computing. Interviewees then revealed that, since there was no regulation related to the security system at the time of interviews, policy makers have the initiative to adopt the provisions on ISO/IEC 27001 as an international security guidance. They also stated that the lack of regulation should not make the business deferred. In fact, policy makers should look for a solution for the technology as a business to be implemented and take the initiative to approach government to advance the regulations to cope with the growth of technology in the business. Interestingly, after the regulation was promulgated, the provision in Ministry Regulation 4/2016[652] stated that, through risk management, electronic system providers should provide a security system for the public service using the guidance in ISO/IEC 27001. Therefore, the government and ICT companies have the same perspective.

The literature related to personal data protection in Chapter 2 reveals that the EU and UK have strictly protection the rights of their citizens' personal data through EU Regulation 2016/679, Directive 2016/680, and Directive 2016/1148.The EU has stated clearly the categories of personal data that should be protected, and the process of

[650]Ibid. (n 149).
[651]Ibid. (n 155).
[652]Ibid. (n 10), Article 2.

protecting it. The promulgation of Ministry Regulation 20/2016 has protected personal data in Indonesia, although it does not mention the categories of personal data that should be protected. This regulation also does not regulate the differentiation of organisations to control and process personal data as the EU did. There is an absence of categorising the data controller and data processor to process personal data in the Regulation.

On studies related to human resource aspects, it was revealed that human resource skill has become one of the aspects of the successful implementation of cloud computing in the companies and business.[653] As stated in ISO/IEC 27001, the company needs to make sure that employees are provided with an understanding of the security system as an aspect in technology. Moreover, EU Directive 97/66/EC[654] states that companies in the telecommunication sectors should take appropriate technical and organisational procedures to support the development of technology itself and the relevant business practices.[655]

This understanding of the security system should be reflected in the life cycle of employment from the recruitment of the employee until the termination of employees. The company needs to make sure that adequate training is provided to improve the skills of employees. Despite the limitations of the training budget, the training itself can be in the form of induction for new staff, on-the-job-training, or annual training. It is also the employees' responsibility to improve themselves so that they have appropriate understanding and knowledge of the latest technology. However, although the implementation of up-to-date technology in ICT companies is essential, there are some employees who do not have the will to improve themselves. To comply with the Indonesian Act of Manpower[656] that prohibits dismissing employees because of skill problems, ICT companies should look for solutions to overcome unskilled employees. Some programmes have been launched by policy makers and were welcomed by employees. The unskilled employees will then be replaced by hiring new professional people who have the knowledge in digital technology in accordance with the corporate

[653]Ibid. (n 73).
[654]Ibid. (n 253), Article 4(1).
[655]Ibid. (n 253), Article 1(1).
[656]Ibid. (n 39), Article 150-172.

strategic plan.

6.3 Research Questions and Findings

One of the aims of the research is to analyse the extent to which the Indonesian cloud computing industry would be affected by wide-ranging data protection and data security law reforms. This research is unique in that it has identified the gap in knowledge relating to the implementation of technology regulations and the development of employer/employee relations in large Indonesian ICT companies. This is the first in-depth study in the area.It has also evaluated the potential impact that data protection and data security law reform could have on the position of employees in the Indonesian cloud computing industry. It focused on evaluating policy makers' perspective that influenced the policy-making in Indonesia's ICT companies. This research also focused on how the policy makers support filling the employees'skills gapsin Indonesia's ICT companies.

The interviews revealed the insights of the policy makers on how cloud computing is being implemented in the company and how employees' skills gaps are being addressed.[657] Deakin[658] stated that empirical legal analysis could be used to support a legal framework as a background of industrial phenomena. Therefore, the methodologies in this thesus us used to see how legal aspects in cloud computing have affected the policy-making process in the Indonesia's ICT companies. To measure the policy makers' perspective, this research interviewed high-level managers who have a role in policy-making in the three biggest companies in the ICT industry in Indonesia.

6.3.1 The extent to which the Indonesian cloud computing industry would be affected by wide-ranging data protection and data security law reforms

The interviews and analysis of the regulations in Chapter 4 have revealed that cloud computing has influenced the ICT industry in Indonesia. The development and implementation of new technology is unavoidable for ICT companies. Cloud computing was implemented in ICT companies years ago; however, since it was implemented, Indonesia has not had specific regulations related to legal aspects in

[657]Ibid. (n 410).
[658]Ibid. (n 409).

cloud computing. In 2016, Indonesia finally has legal certainty on legal aspects of cloud computing by the promulgation of ISMS and Protection of Personal Data in the Electronic System regulations in 2016. Those regulations have supported ICT companies in protecting security systems and personal data. According to the interview in Section 4.3.1, before the promulgation of those regulations, ICT companies were using ISO/IEC 27001 as an international guidance in the security system to fill up the implementation period of the regulations and the policy makers approached the regulator to put some provisions of ISO/IEC 27001 as guidance in the ISMS regulation. With the promulgation of ISMS regulation, ICT companies need to make sure that they already comply with the provisions in the regulations, including to make sure that all of the employees are already aware of the up-to-date security system in the companies.

Related to the Protection of Personal Data in the Electronic System regulations, it needs to be clear what kind of data is included in the definition of personal data. To avoid confusion, the government needs to release a statement related to the kind of data that can be classified as personal. Indonesian regulations also do not recognise the terms data controller and data processor. The DPA,[659] EU Directive 2016/680,[660] and EU Regulation 2016/679[661] have emphasised clearly which legal person or public authority or agency or other body has a responsibility as data controller and data processor. A clear perspective on who will be responsible as the person or body to act as data controller or data processor will give a legal certainty for Indonesian ICT companiesandthe cloud customer. It will clarify who will protect their personal data, and it will clarify the role and obligation of ICT companies in relation to controlling and processing data in their premises.

This thesis is suggesting the establishment of a national organisation supervised by the Ministry of Communication and Information Technology to support the protection of security and data protection in Indonesia. The form of this national organisation might besimilar to the EDPB[662] or Data Protection Office.[663] It will act as the representative

[659]Ibid. (n 278), Section 1(1).
[660]Ibid. (n 27), Article 3(8,9).
[661]Ibid. (n 26), Article 4(7,8).
[662]Ibid. (n 26), Article 68.

of government on behalf of data subjects, including the industry. Like the European bodies, the role of this national organisation will be to make sure that ICT companies fulfil the provisions related to data protection principles and advise on the security of personal data. Therefore, the establishment of the national organisation will give legal certainty on data security and the protection of personal data, but also educate the citizens on the importance of those protections. This reform will contribute to the growth of the cloud computing industry in Indonesia.

6.3.2 The potential impact that data protection and data security law reform could have on the position of employees in the Indonesian cloud computing industry.

The interviews showed that employees should keep updated on the newest technology that is implemented and marketed in the company. Policy makers as leaders should set an example. The interviews showed that policy makers did encourage their staff to maximise the technology in their role. They suggested that there should be an ecosystem to support each employee in the implementation of cloud computing. However, this ecosystem should also consider the legal aspects, not merely the technological.[664] Employees' understanding should cover the impact of the changes, especially regarding data security, personal data protection, and data controllers and data processors. Policy makers should be aware of the legal consequences if cloud computing is not well implemented. Cybercrime is likely to happen if employees who have the authority to access the system become corrupt.[665]

The required awareness can be obtained through training provided in the companies, as required by the Indonesian Manpower Act[666] and EU Directive 97/66/EC.[667] Those two regulations emphasise that, in ICT companies, it is required for all employees to be aware and keep up-to-date with the issues and risk related to information security and to make sure that they protect the personal data. This means the employers have a responsibility to provide regular, appropriate training, and budgetary considerations

---

[663]Ibid. (n 26), Article 37-39.
[664]Ibid. (n 54).
[665]Ibid. (n 37).
[666]Ibid. (n 39), Article 12(1).
[667]Ibid. (n 253), Article 4(1).

should not outweigh this need.

Therefore, policy makers should also be aware of those areas and give consideration to the treatment of data security and personal data in policy-making. They need also to make sure that all employees are up-to-date with security, and this can be achieved through the annual signing of an integrity pact which challenges the awareness of employees regarding integrity, business ethics and confidentiality.

ICT companies also have to make sure that they have protected the employees' personal data throughout the cycle of employment, and policy makers could ask the government to make provision in the regulation in this area.

Policy makers need to make sure that employees are prepared to meet the challenge of the companies' strategic plan and so ICT companies need qualified employees. Policy makers should have a plan for the employment cycle. Employees need to support the companies' strategic plan and be digitally literate. However, not all have the ability or willingness to exist in the digital world. As the Indonesian Act of Manpower does not allow dismissal related to skill problems, policy makers should figure out a solution to overcome this. One of the solutions is through an exit system called the golden and silver handshake. Those solutions have proved to be acceptable by all employees and are not against manpower regulations.

The implementation of cloud computing is not only shifting the employees' habits, but also has another consequence related to data security and data protection, which is they need to be aware of those aspects of protection. ICT companies will transform the recruitment system by adding digital literacy as a requirement and will replace reluctant employees with professional peoplewith knowledge of technology. Therefore, employees need to improve themselves, so they can meet the requirements of the digital world.

6.4 Strengths and Limitations of the Research

This research has some strengths and limitations that arise from the methods used to analyse the literature reviews and interviews from the participants.

6.4.1 Strengths

This research has several strengths related to the interviewees, the outcome of the

research, and the up-to-date regulations in Indonesia.

Interviewees

The policy makers interviewed for this thesis were senior management with expertise and experience in their field, and who could approve drafts of policy before it was approved by the directors in the company. This is unprecedented access to policymakers in a unique institution, firstly because the researcher is the employee of the company which has funded the research, and also because policy makers were directly chosen by the relevant director. The institutions were also unique because the research was conducted in the biggest state-owned company in Indonesia and its subsidiaries.

The researcher gained unique access by being an employee of one of the companies and the companies themselves have given support to the research. Therefore, the result of the interviews of this thesis is original and unique because the researcher is studying phenomena that are currently occurring in her own workplace. The interviewees were chosen because they had capacity in policy-making relevant to the subject matter of the thesis. All were in positions at the strategic managerial level in legal, IT and employment divisions.

According to their annual report,[668] the ICT companies in this research recorded a net profit in 2015 of $1.17 billion, which is a 7% increaseon 2014. The company, through its subsidiaries, has over 150 million mobile users and growth of 43.9% in digital business data and 39.2% in digital services. With the huge responsibility to retain customers by improving its quality of service, policy makers play a big role in formulating the business and employee policies.

Real situations related to decision making in Indonesia's ICT companies could be discerned through the interview results. The interview findings are adequate and satisfying to describe the policy-making process in the state-owned ICT company and its subsidiaries. With the specific policy makers' expertise, this research focused on the policy makers' perspective in the legal aspects in cloud computing in improving employees' skills. Using content analysis revealed the selective, valid, and reliable

[668]Ibid. (n 434).

perspective of policy makers to develop the code in constructing the analysis.[669]

The fact that this research was held in a state-owned company enriches the results, as there are different treatments in some business areas that make the company subject to the regulations related to state-owned companies. However, the development of technology is implemented in most sectors in Indonesia,[670] including government institutions.[671] Therefore, to make sure that regulation covers the implementation of technology, it is important not only for companies, but also other institutions to be regulated by effective laws.

Focus on legal aspects incloud computing

This research focused on data security, personal data protection, data controllers and data processors in cloud computing,which is vitally important to ICT companies. EU, UK, and Indonesian regulations and policies were examined from the policy makers' perspective on legal aspects in cloud computing in the policy-making process.[672] The fact that technology use has become habitual[673] would bring certain considerations that employees should be aware of the effect of the implementation of technology and the legal aspects implied in it. At the time when the interviews were conducted, there was no regulation that covered these aspects. The regulations were published in 2016, but some areas need to be strengthened to provide comprehensive protection. These considerations can only properly be addressed by experts such as the policy makers in this study.

Highlighting up-to-date Indonesian Regulation on ICT

This research highlighted the Indonesian regulations promulgated in 2016. The interviews were conducted in 2015, before the data security and personal data regulations were promulgated. Therefore, it depicted the real conditions in ICT companies before the regulations were promulgated. The companies' effort to promote the implementation of data security was kept in line with provisions on data

[669]Ibid. (n 411).
[670]Ibid. (n 354); Ibid. (n 356)
[671]Ibid. (n 358).
[672]Ibid. (n 39).
[673]Ibid. (n 94).

security regulation by implementing ISO/IEC 27001 as security guidance.[674] However, some considerations still have not been regulated yet, related to the data controllers and data processors. Like the EU and UK, there should be clear responsibility of organisations that handle data protection.[675] Segura-Serrano[676] stated that a regulatory approach would confirmthe obligation to data security. Indonesian regulations on personal data protection state that there will be an educational campaign related to the implementation of the regulation of personal data.

It could be the government's intention to have a comprehensive regulation to give legal certainty in the implementation of personal data protection. This research enriched the literature on policy makers' strategy during the implementation period to obtain legal protection that can be used to support the business and see how the regulation copes with the development of technology in Indonesia.

Enactment of National regulator

This research has suggest the enactment of national regulator to support the promulgated of personal data protection regulation. The role of this body is similar to the role and obligation of EDPB under EU's General Data Protection Regulation, which is to make sure the Indonesia, has strong law enforcement through national supervisory. Indonesia should have a statutory obligation to comply with data protection and security laws, and failure to do so could lead to breach the law which national regulator could enforce. This body is supervised by Minister of Ministry of Communication and Information Technology, and it has the role to oversee and to make sure that personal data regulation is well implemented and to create a good collaboration between Minister of Ministry of Communication and Information Technology and ICT industry. Since personal data regulation is relatively new in Indonesia, the existence of this body will support the implementation of personal data protection in Indonesia, and regulator had to make sure that Indonesian citizen had already aware and understand the right and responsibilities in personal data protection and data security. The enactment of this body will also to support the economic

[674]Ibid. (n 10), Article 7.
[675]Ibid. (n 278), Section 1 (1); Ibid. (n 27), Article 3 (8, 9); Ibid. (n 26), Article 4 (7, 8).
[676]Ibid. (n 559).

partnership between EU and EEA with Indonesia since Indonesia has the equal protection in personal data and data security.[677]

6.4.2 Limitations

The research has a number of limitations, which are discussed below.

Participants

The participants in this research were from three companies, which have been selected based on the accreditation in 2015 by The Indonesian Central Bureau of Statistics.[678]It therefore reflects only the views of participants from the three biggest state-owned Indonesian ICT companies. Although the interviewees were limited to those companies, the findings can be applied to most ICT companies in Indonesia, since the participants were selected from all the relevant personnel at the decision-making level in each company.To make the results more comprehensive, further research with participants from smaller companies and ones not subject to the Law on State-Owned Enterprises should be conducted, and different typesof industry, such as banks, public services or airlines company might enrich the findings.

Funded research

The companies accessed in this research also funded the research itself. Furthermore, the researcher is also an employee of one of the funding companies. This research probed the issues using examples from these funded companies. The research carried out gained full approval from Lancaster University's Ethics Committee and all recommendations were followed.

Employee participation

This research has its focus on policy makers and any opinions raised from employees' perspectiveswere not exposed. To investigate whether the implementation of policy related to technology in the company was successful and had the desired effect for the development of employees' skill in the company, there should be insight from the

---

[677]Ibid (n 26), Art. 46

[678]'Statistics of Information and Communication, 2015' (*BPS-Statistics Indonesia*, 2015) <https://www.bps.go.id/website/pdf_publikasi/Statistik-Perusahaan-Informasi-dan-Komunikasi-2015.pdf> accessed 15 July 2016.

employees' perspective in future research.

Directors'participation

The policy makers had to align their policy to the company's strategic scenario, which would be ratified by the directors. Therefore, perspective from the director related to the policy draft will enrich the policy itself. To investigate whether the policy is consistent with the company's strategic scenario, and whether the director had agreed with the policy itself, it is necessary to have some input from the directors of the company. Further research on their involvement in policy-making may enrich the findings of future research on the company's support for the improvement of employees' skills.

6.5 Contributions

This research contribution is to the implementation of the legal aspects in cloud computing in ICT companies. Using empirical legal research, it examined the implications of cloud computing phenomena relation to policy-making in ICT companies. Policy makers' perspectives were obtained from interviews and analysed through classical content analysis. It used to compare the policy and regulations of the EU, UK, and Indonesia. All the data collected in this research has been used to draw meaningful conclusions on the implementation of the legal aspects in cloud computing in ICT companies.

Previous literature related to cloud computing classified the implications of the implementation of cloud computing related to networks, servers, storage and applications that were moulded into a service.[679] Studies have classified the crucial aspects of the implementation of cloud computing as a business model in the company. Beside the technological infrastructure issues, data security and privacy have become the users' main concerns in cloud computing (see Chapter 2). Therefore, this research has highlighted the importance of data security, personal data protection, and data controllers and data processors in relation to policy-making on the development of employees' skills. It discussed the importance of regulatory protection

[679]Ibid. (n 46).

and to what extent policy makers' perspective on employees' skills development could overcome the growth of technology. Hence, this research contributes to supporting the growth of employees' skills and understanding and the growth of cloud computing in Indonesia.

The review of the legal aspects of cloud computing has revealed that Indonesia's regulations provide protection related to data security and personal data through Ministry Regulations 4/2016 and 20/2016 which cover the security system and the protection of personal data. However, they do not define personal data, unlike the EU and UK regulations. This could introduce bias on the responsibility of protecting the personal data by provider. Therefore, this research contributes to the literature by confirming the lack of classification of personal data in Indonesian regulation. Indonesian laws need to be improved to match the levels of the EU and UK. This research also states the importance of the protection of employees' personal data. Therefore, this research contributes to the literature by confirming the lack of personal data protection in Indonesia.

The review of data controller and data processor functions has also revealed that the Indonesian regulations do not recognise the separation and classification of organisations to control and process personal data as is the case in the EU and UK. It can be seen fromthe lack of provision in the Regulations related to the different organisations; although one provision in Government Regulation 82/2012[680] states that ESOs could delegate the electronic transaction to an electronic agent. An electronic agent, according to Government Regulation 82/2012,[681] is a device or an electronic system to perform an electronic transaction. However, after delegation, ESOs do not have responsibility for the data. This transaction would have eliminated the responsibility of ESOs in protecting personal data in the electronic transaction. The unclear responsibility could lead to legal uncertainty. Therefore, this research also contributes to the literature by confirming the lack of classification of data controller and data processor in Indonesian regulation.

It should be borne in mind that Indonesia has promulgated its regulation in data

[680]Ibid. (n 253), Elucidation.
[681]Ibid. (n 253), Article 1(3).

protection in 2016, therefore, Indonesia has a lot to learn from the GDPR, not only in terms of world leading laws, but also, in terms of how alignment with EU law would help strengthen economic cooperation, moreover, in the GDPR, it is prohibits to transfer personal data to countries that do not provide an adequate or equivalent level of data protection.[682]

At the moment, Indonesian company is relying on standard contractual clauses to comply with GDPR in the respect of processing any partnership in EU or EEA. In the longer-term (as it secures more EEA based work) this is not a cost effective approach. New contractual clauses would have to be drafted for each new processing contract entered into. Also, complying with two or more sets of legal standards is administratively burdensome so there is a rationale for Indonesian law matching the high standards in the GDPR. For this reason, the Indonesian government should also consider seeing either a whole country (for example Japan/ sector specific adequacy decision like Privacy Shield) to make EEA – Indonesian data legally easier and more cost effective. But, an adequacy decision will not be forthcoming unless Indonesian law closely mirrors the GDPR. This includes provisions concerning the role of the regulator, the rights and responsibilities of data subjects, data controllers and data processors.

As stated previously, Indonesian government has and encourage having strong economic ties with the EU/ EEA, which requires an essential equivalent level of data protection and data security, therefore, Indonesia should strengthen their regulation in such areas. The enforcement of GDPR has brought some lesson learned in terms of world leading laws and also how to synchronise with the EU law to strengthen the economic links between Indonesia and EU/ EEA, especially in terms of personal data protection, data controller, data processor, transferring personal data to other countries, and also to have supervisory and enforcement powers to monitoring, advisory, guiding, recommending, as well as reviewing the implementation of GDPR and to make sure that the personal data protection regulation is applied correctly.

Another importance to have an equivalent level of data protection and data security as

---

[682]Ibid. (n 26), Art. 44

EU/ EEA is when the companies would like to expand its subsidiaries in such countries that ratify the GDPR. The companies require complying with the law that lies in the country. It will become a burdensome for the company to have to comply with more than one set of data protection and data security in all locations in EU. Therefore, it is best for Indonesia for adopting the highest (GDPR) standards and applying those rules in GDPR.

The qualitative approach through interviews of policy makers also contributed insights into how companies support employees' development in technology and skills. Policy makers stated that companies already educate employees from the induction programme until termination. Those policies are in line with the guidance on ISO/IEC 27001 and the provisions of EU Directive 97/66/EC. However, despite there being a budget obstacle to conducting training, there should be a continuous learning process concerning security and data protection. Employees should have an understanding of the security system and its updates. To support this, policy makers should produce policy related to security management, and hence this research contributes to supporting policy makers by making sure that they consider security training, as required by ISO/IEC 27001. The interviews also reveal what solution policy makers have developed to overcome employee resistance to the implementation of new technology. They stated that exit programmes benefit both employee and company.

This research was conducted in the state-owned ICT company and its subsidiaries. Therefore, it gives perspectives on how the company manages its business based on SOE Law,[683] the Limited Liability Companies Act,[684] and the regulations of the New York Stock Exchange and Indonesia Stock Exchange. This research has contributed a unique outlook that described how this company conducts its business.

Overall, this research has contributed significant input to reviewing Indonesian regulations related to the development of cloud computing and employees' positions in ICT companies. To supervise the implementation of legal aspects as discussed in this research, it is necessary for the Indonesian government to establish a national organisation to support comprehensive protection and public information for

[683]Ibid. (n 432).
[684]Ibid. (n 433).

Indonesian citizens in the era of cloud computing, especially for the protection of personal data. Clear provisions will promote legal certainty in cloud computing.

Further research on the implementation of data security and data protection in ICT companies in Indonesia needs to be focused on the two aspects: the legal and the organisational.

The main object of legal studies should be to identify the potential ways of improving the implementation of data security and data protection policies and compliance with regulations in Indonesia. The focus of the studies should include identifying personal data and sensitive personal data; identifying the role of data controller and data processor in the company; and the potential impact of the establishment of a national organisation on data security and data protection. It could also provide profiles of companies in a different scale of businesses and different type of industries.

The selection of policy makers as interview subjects in this thesis is important because they have the authority to make strategic policy in the company. Further studies on the employee aspects could provide insight for commentators and policy makers, to determine whether the company policies are appropriately implemented and well-executed.

6.6 Conclusion

The aim of the research was to analyse the extent to which the Indonesian cloud computing industry would be affected by wide-ranging data protection and data security law reforms, through interviews and legal review. It found that the Indonesian government should reform the Ministry Regulations on security to promote data security. Lack of definitions of personal data and sensitive personal data will potentially create different interpretations, which might lead to failure of protection. Lack of protection of employees' personal data is also highlighted; such protection throughout the cycle of employment will provide a good environment in the workplace.

Unclear responsibilities borne by ESOs and electronic agents might cause uncertainty over responsibility between them, which might lead to a potential loss of personal data.

This understanding of legal aspects is important for employees in ICT companies and should be facilitated by the company to avoid a failure in protection of personal data of customers and employees and company data. Continuous learning should be available to employees to improve their understanding of the protection of personal data. Insight from the employees might contribute positive feedback for policy makers in supporting the development of employees'skill.

The government, through a new national organisation, should ensure that protection related to data security and personal data complies with the regulations and has been properly implemented by ESOs and electronic agents.

The outcome from this research thesis has shown that it is necessary for policy makers and employees of ICT companies in Indonesia to be aware of the development of technology, not only from the technology perspective, but also from the impact of its development. Security and the protection of data is key to this. Policy makers and employees should be able to treat data security and personal data equally in terms of the protection of customer data, corporate data, and the employees' data in the company.

The perception that comes from policy makers in ICT companies might contribute to what extentthey and the employees consider the importance of data security and personal data protection. The findings should support the Indonesian government's efforts in the development of technology to make the technology applicable and lawful. It also helps the policy makers align the development of technology, the development of the company's employees, and compliance with regulation.

The Indonesian government should support the development of technology and business through regulation of data security and data protection and of data controllers and data processors. This will benefit not only business, but also the customers of cloud computing. Government should make a clear regulation to avoid misinterpretation of the information by the public. To be effective, this will have to include public education on the implications of cloud computing in Indonesia. A comprehensive regulation will not only protect citizens as customers, but also will protect them as employees. The government should encourage the business players to continually improve the skill of their employees to overcome skills gaps. Given the level of technology misuse, the government needs to make a stronger regulations, like

those of the EU and UK, to protect businesses, consumers and employees.

References

Table of Cases

UK Cases

Tiptools Limited v T W Curtis [1973] IRLR 276.

E C Cook v Thomas Linnell & Sons Limited[1977] IRLR 132

Taylor v Alidair Limited [1978] IRLR 82

R v Sunderland (unreported) 20 June 1983.

DPP v Bignell [1988] 1 Cr App R 1.

Denco Ltd v Joinson [1991] IRLR 63.

DPP v McKeown, *DPP v Jones* [1997] 2 Cr.App. R. 155, HL

R v Gold &Schifreen (1988) 1 AC 1063

R v Sheppard [2001] EWCA Crim 65

Pickersgill v Employment Service [2002] EWCA Civ 23.

R v Smith (Wallace Duncan) (No. 4) [2004] EWCA Crim 631 Q.B 1418

R v Crosskey (Gareth) [2012] EWCA Crim 1645; [2013] 1 Cr.App.R.(S) 76

R v Mangham (Glen Steven [2012] EWCA Crim 973; [2013] 1 Cr.App.R.(S) 11

Arthur J. Gallagher Services (UK) Limited and others v Skriptchencko and others [2016] EWHC 603 (QB)

Mark Lloyd case in 2016

Shamim Sadiq case in 2017

Kevin Bunsell case in 2017

Vote Leave Limited [2018] EWHC 2414 (Admin)

R v Mudd [2018] 1 Cr App R (S) 33 (7)

European Cases

European Court of Justice: C-362/14-Schrems.

Table of Legislation

Table of Legislation: EU

EU Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 On the Protection of Individuals with Regard to The Personal Data and On the Free Movement of Such Data.

EU Directive 97/66/ECconcerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.

EU Directive 2002/58/EC of The European Parliament and of The Council of 12 July 2002 Concerning the Processing of Personal Data and The Protection of Privacy in The Electronic Communications Sector (Directive on Privacy and Electronic

Communication).

EU Directive 2009/136/EC of the European Parliament and of the Council Of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services.

EU Directive 2016/680 on The Protection of Natural Persons with Regard to The Processing of Personal Data by Competent Authorities for The Purposes of The Prevention, Investigation, Detection or Prosecution of Criminal Offences or The Execution of Criminal Penalties, And on The Free Movement of Such Data, And Repealing Council Framework Decision 2008/977/JHA.

EU Directive 2016/1148 on Measures for A High Common Level of Security of Network and Information Systems Across the Union.

EU Regulation 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws.

EU Regulation 2016/679 of The European Parliament and of The Council of 27 April 2016 on The Protection of Natural Persons with Regard to The Processing of Personal Data and On the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

EU Report 2013/2063(INI) on Unleashing the Potential of Cloud computing in Europe.

European Treaty Series - No. 108on Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Table of Legislation: UK

Data Protection Act (DPA) 1984

Computer Misuse Act (CMA) 1990.

Data Protection Act (DPA) 1998.

Employment Rights Act 1996.

Employee Study and Training (Procedural Requirements) Regulation 2010.

Employment Rights Act 1996.

Table of Legislation: Indonesia

Indonesian Act 13/2003 regarding Manpower.

Indonesian Act 14/2008 regarding Public Information Disclosure Act.

Indonesian Act 40/2007 regarding Limited Liability Company.

Indonesian government Regulation 47/2012 regarding Social and Environmental Responsibility of Limited Liability Company

Indonesian government Regulation 82/2012 regarding Implementation of Electronic System and Transactions.

Indonesian Law 10/2004 regarding Establishment of Legislation.

Indonesian Law 11/2008 regardingElectronic Information and Transactions.

Indonesian Law 19/2003 regarding State-Owned Enterprises.

Indonesian Ministry Regulation 4/2016 regarding ISMSs.

Indonesian Ministry Regulation 8/2014 regarding Competency Based Management Training.

Indonesian Ministry Regulation 20/2016 regarding Data Protection in Electronic System.

Indonesian Ministry Regulation 26/PER/M.KOMINFO/5/2007 regarding On Securing the Making Use of Internet Protocol Based Telecommunication Network.

Indonesian Ministry Regulation 29/PER/M.KOMINFO/12/2010 regarding Second Amendment to The Decree of The Minister of Communication and Information Technology Number 26/Per/M.Kominfo/5/2007 On Securing the Making Use of Internet Protocol Based Telecommunication Network.

Indonesian Ministry Regulation PER-05/MBU/2007 regarding Partnership Program State-Owned Enterprises with Small Business and Environtment Program

Indonesian Presidential Decree 53/2017 regarding Indonesian Cyber Agency and National Encryption Agency.

Indonesian Presidential Instruction 6/2001 regarding Information and Communication Technology.

Bibliography

'About The DPA 2018' (*Ico.org.uk*, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/> accessed 22 April 2019

ACAS A, 'Code of Practice on Disciplinary and Grievance Procedures' (Advisory, Conciliation and Arbitration Service, 2015) <http://www.acas.org.uk/media/pdf/f/m/Acas-Code-of-Practice-1-on-disciplinary-and-grievance-procedures.pdf> accessed 11 March 2016.

Amato F and others, 'Improving Security In Cloud By Formal Modeling Of Iaas Resources' (2018) 87 Future Generation Computer Systems

Abramowicz W, *Business Information Systems Workshops* (Springer 2014).

Acquisti A, Friedman A and Telang R, 'Is There a Cost to Privacy Breaches? An Event Study', *International Conference on Information Systems* (2006) <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf> accessed 1 September 2016.

Adamiak M, Apostolov A, Begovic M, Henville C, Martin K, Michel G, Phadke A and Thorp J, 'Wide Area Protection—Technology and Infrastructures' (2006) 21 IEEE Transactions on Power Delivery .

Aguinis H and Kraiger K, 'Benefits of Training and Development for Individuals and Teams, Organisations, and Society' (2009) 60 Annual Review of Psychology.

Aiyer G, 'Global Investment Community Can't Afford to Ignore Sustainability' (the Guardian, 2014) <http://www.theguardian.com/sustainable-business/2014/nov/14/global-finance-community-principles-responsible-investment> accessed 18 November 2014.

Alsmadi DV Prybutok, 'Sharing and Storage Behaviour Viacloud: Security and

Privacy in Research and Practice' (2018) 85 Computers in Human Behavior.

Anthony R, *Planning and Control Systems* (1st edn, Division of Research, Graduate School of Business Administration, Harvard University 1981).

Arendt L, 'Barriers to ICT Adoption in SMEs: How to Bridge the Digital Divide?' (2008) 10 Journal of Systems and Information Technology.

Armbrust M, Stoica I, Zaharia M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D and Rabkin A, 'A view ofcloud computing' (2010) 53 Communications of the ACM.

Arnold C, 'Funding: NIH Grants Fund Technology Development' (2013) 382 the Lancet.

Asian Development Bank, 'Promoting Information and Communications Technology in Indonesia' (ADB Indonesia Resident Mission 2015).

Baldwin C, Arturo Garza-Reyes J, Kumar V and Rocha-Lona L, 'Personal Development Review (PDR) Process and Engineering Staff Motivation' (2014) 25 Journal of Manufacturing Technology Management.

Bapna R, Langer N, Mehra A, Gopal R and Gupta A, 'Human Capital Investments and Employee Performance: An Analysis of IT Services Industry' (2013) 59 Management Science.

Barzegar N and Farjad S, 'A Study on the Impact of On the Job Training Courses on the Staff Performance (A Case Study)' (2011) 29 Procedia - Social and Behavioural Sciences.

Basu A, Vaidya J, Kikuchi H, Dimitrakos T and Nair, S K,'Privacy Preserving Collaborative Filtering for Saas Enabling PaasThe clouds' (2012) 1 Journal ofcloud computing: Advances, Systems and Applications.

Bauer E and Adams R, *Reliability and Availability ofcloud computing* (Wiley-IEEE Press 2012).

Bel B, V Smirnova Wait, 'Managing Change: Communication, Managerial Style and Change in Organisations' (2018) 69 Economic Modelling.

Benn S and Bolton D, *Key Concepts in Corporate Social Responsibility* (SAGE 2011).

Bhardwaj S, Jain L and Jain S, 'Cloud computing: A Study of Infrastructure as A Service (Iaas)' (2010) 2 International Journal of Engineering and Information Technology.

Bhatt D, 'A Revolution in Information Technology -cloud computing' (2011) 9 Walailak Journal of Science and Technology (WJST) <http://wjst.wu.ac.th/index.php/wjst/article/view/25/203> accessed 10 May 2015.

Black H, Nolan J and Nolan-Haley J, *Black's Law Dictionary* (West 1990).

Blowers M, *Evolution of Cyber Technologies and Operations To 2035* (1st edn, Springer International Publishing 2015).

Blowfield M and Murray A, *Corporate Responsibility* (Oxford University Press 2008).

Bodei C, Degano P, Galletta L, Mezzetti G and Ferrari G, 'Security in Pervasive Applications: A Survey' (2013) 4 European Journal of Law and Technology

<http://ejlt.org/article/view/276> accessed 10 October 2015.

Boehm F, Hey T and Ortner R, 'How to Measure IT Security Awareness of

Bonk C, 'Online Training in An Online World' (2002) 16 USDLA Journal.

Boockmann B, J FriesC Göbel, 'Specific Measures For Older Employees And Late Career Employment' (2018) 12 The Journal of the Economics of Ageing

Boukerche AR De Grande, 'Vehicularcloud computing: Architectures, Applications, And Mobility' (2018) 135 Computer Networks.

BPS, 'Population 15 Years of Age and over Who Worked during the Previous Week by Main Employment Status and Main Industry, 2008 - 2017' (*Bps.go.id*, 2017) <https://www.bps.go.id/statictable/2016/04/05/1911/penduduk-berumur-15-tahun-ke-atas-yang-bekerja-selama-seminggu-yang-lalu-menurut-status-pekerjaan-utama-dan-lapangan-pekerjaan-2008---2017.html> accessed 21 December 2017.

BPS. 'Statistics of Information and Communication, 2015' (*BPS-Statistics Indonesia*, 2015) <https://www.bps.go.id/website/pdf_publikasi/Statistik-Perusahaan-Informasi-dan-Komunikasi-2015.pdf> accessed 15 July 2016.

Briscoe G and Marinos A, 'Digital Ecosystems in the clouds: Towards Communitycloud computing', *3rd IEEE International Conference on Digital Ecosystems and Technologies* (Institute of Electrical and Electronics Engineers (IEEE) 2009).

Buyya R, Yeo C s, Venugopal S, Broberg J, and Brandic I, 'Cloud computing and Emerging IT Platforms: Vision, Hype, And Reality for Delivering Computing As the 5Th Utility' (2009) 25 Future Generation Computer Systems.

Caerteling J S, Halman J I M, Song M, Doree A G and Van Der Bij H, 'How Relevant Is Government Championing Behaviour in Technology Development?' (2012) 30 Journal of Product Innovation Management.

Calder A, *ISO27001* (IT Governance Publishing 2013).

Cane P and Kritzer H, *The Oxford Handbook of Empirical Legal Research* (1st edn, Oxford University Press 2010).

Cardona M, Kretschmer T and Strobel T, 'ICT and Productivity: Conclusions from the Empirical Literature' (2013) 25 Information Economics and Policy.

Carey P and Carey P, *Data Protection* (Oxford University Press 2009).

Carraher S, 'Turnover Prediction Using Attitudes towards Benefits, Pay, and Pay Satisfaction among Employees and Entrepreneurs in Estonia, Latvia, and Lithuania' (2011) 6 Baltic Journal of Management.

Carrieri MCarrieri, M., Crete-Nishihata, M., Dalek, J., Deibert, R., Haselton, B., Khan, S., Lau, M., Noman, H., Poetranto, I., Senft, A., Wiseman, G., Marquis-Boire, M., Marczak, B. and Scott-Railton, J, 'Islands of Control, Islands of Resistance: Monitoring the 2013 Indonesian IGF' (Citisen Lab at the Munk School of Global Affairs, University of Toronto 2014) <https://citisenlab.org/2013/10/igf-2013-an-overview-of-indonesian-internet-infrastructure-and-governance/> accessed 5 October 2015.

Carroll M, van der Merwe A and Kotze P, 'Securecloud computing: Benefits, Risks and Controls' [2011] 2011 Information Security for South Africa.

Casola V De Benedictis, A., Rak, M. And Villano, U, 'Monitoring data securityinthe cloud: A security SLA-based approach' [2018] Security and Resilience in Intelligent Data-Centric Systems and Communication Networks.

Castro C, Reed C and Queiroz R, 'On the Applicability of The Common European Sales Law to Some Models ofcloud computing Services' (2013) 4 European Journal of Law and Technology <http://ejlt.org/article/view/186/409> accessed 5 August 2016.

Castro Silva HF Lima, 'Technology, Employment and Skills: A Look into Job Duration' (2017) 46 Research Policy.

CayirciE, GARAGA, A., SANTANA DE OLIVEIRA, A. and ROUDIER, Y, 'A Risk Assessment Model for Selecting The cloud Service Providers' (2016) 5 Journal ofcloud computing.

Cearley D, 'Cloud computing - Key Initiative Overview' (*Gartner.Inc*, 2010) <https://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_The cloudComputing.pdf> accessed 12 February 2015.

Chana I and Kaur T, 'Delivering IT as A Utility- A Systematic Review' (2013) 3 International Journal in Foundations of Computer Science & Technology.

Chandler P, *An A-Z of Employment Law: A Complete Reference Source for Managers* (4th edn, Kogan Page Ltd 2003).

Chaulya SG Prasad, 'Application ofcloud computing Technology in Mining Industry' [2016] Sensing and Monitoring Technologies for Mines and Hazardous Areas.

Chesley N, 'Technology Use and Employee Assessments of Work Effectiveness, Workload, and Pace of Life' (2010) 13 Information, Communication & Society.

Chen W and Xu R, 'Clean Coal Technology Development in China' (2010) 38 Energy Policy.

Chow R, Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. and Molina, J,'Controlling Data in the cloud' [2009] Proceedings of the 2009 ACM workshop on cloud computing security - CCSW '09.

Chua H N., Herbland, A., Wong, S. F. and Chang, Y,'Compliance to Personal Data Protection Principles: A Study of How Organisations Frame Privacy Policy Notices' (2017) 34 Telematics and Informatics.

Chua, H. N., Wong, S. F., Low, Y. C. and Chang, Y, 'Impact of Employees' Demographic Characteristics on The Understanding and Compliance of Information Security Policy in Organisations' (2018) 35 Telematics and Informatics.

'Consultative Committee of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data' (*Rm.coe.int*, 2019) <https://rm.coe.int/observers-state-of-play-and-admission-criteria/16808fdc4d> accessed 10 April 2019.

Cohen D and Crabtree B, 'RWJF - Qualitative Research Guidelines Project | Semi-Structured Interviews | Semi-Structured Interviews' (Qualres.org, 2006) <http://qualres.org/HomeSemi-3629.html> accessed 13 March 2015.

Collin P, *Dictionary of Law* (A & C Black 2007).

Colquitt J, J LePineR Noe, 'Toward an Integrative Theory of Training Motivation: A

Meta-Analytic Path Analysis Of 20 Years of Research'. (2000) 85 Journal of Applied Psychology.

Columbus L, 'The Bestcloud computing Companies and CEOs to Work for in 2015' (Forbes.com) <http://www.forbes.com/sites/louiscolumbus/2015/01/29/the-best-the cloud-computing-companies-and-ceos-to-work-for-in-2015/> accessed 10 October 2016.

Conti G, 'Training, Productivity and Wages in Italy' (2005) 12 Labour Economics.

Coovert M and Thompson L, *The Psychology of Workplace Technology* (Routledge 2014).

Costa, P., Migliavacca, M., Pietzuch, P. and Wolf, A. L, 'Naas: Network-As-A-Service in The cloud', *2nd USENIX Workshop on Hot Topics in Management of Internet, The cloud, and Enterprise Networks and Services* (USENIX 2012) <https://www.usenix.org/conference/hot-ice12/naas-network-service-the cloud> accessed 13 February 2016.

Cryer R and others, *Research Methodologies in EU and International Law* (1st edn, Hart Publishing 2011).

D. Brickley 2nd S and M. Gottesman B, 'Business Law Basics' (Businesslawbasics.com, 2016) <http://www.businesslawbasics.com/business-law-basics> accessed 5 October 2015.

D'Arcy J and Devaraj S, 'Employee Misuse of Information Technology Resources: Testing A Contemporary Deterrence Model' (2012) 43 Decision Sciences.

Dachyar M and Prasetya M, 'Cloud computing Implementation in Indonesia' (2012) 2 International Journal of Applied Science & Technology.

Dane F, *Evaluating Research* (1st edn, Sage 2011).

'Darren Harrison' (*Ico.org.uk*, 2019) <https://ico.org.uk/action-weve-taken/enforcement/darren-harrison/> accessed 11 April 2019

de Hert P, V PapakonstantinouI Kamara, 'Thecloud computing Standard ISO/IEC 27018 Through the Lens of The EU Legislation on Data Protection' (2016) 32 Computer Law & Security Review.

Denscombe M, *The Good Research Guide for Small-Scale Social Research Projects* (1st edn, Open Univ Press 2007).

Dillon T, Wu C and Chang E, 'Cloud computing: Issues and Challenges' [2010] 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

Dinh H and others, 'A Survey of Mobilecloud computing: Architecture, Applications, and Approaches' (2011) 13 Wireless Communications and Mobile Computing.

Dixon B and others, *A Handbook of Social Science Research* (1st edn, Oxford University Press 1992).

Employees: A Comparison to E-Mail Surveillance at The Workplace' (2016) 7 European Journal of Law and Technology <http://ejlt.org/article/view/500/634> accessed 2 September 2016.

European Commission, 'Employment Package - Employment, Social Affairs & Inclusion - European Commission' (*European Commission*, 2018)

<http://ec.europa.eu/social/main.jsp?catId=1039&langId=en> accessed 28 June 2018.

Erl, T, *Cloud computing: Concepts, Technology, & Architecture* (1st edn, Pearson Education (US) 2013).

EU-Indonesian Business Network, 'Indonesian ICT Market' (Your Gateway to Indonesia 2015) <http://www.eibn.org/upload/EIBN_Presentation_ICT_Indonesia.pdf> accessed 23 June 2016.

EU Indonesia Business Network, 'Your Gateway to Indonesia' (*EIBN (EU Indonesia Business Network)*, 2015) <http://www.eibn.org/upload/EIBN_presentations_for_companies_2015_small.pdf> accessed 11 February 2017.

European Commission, 'Annual Growth Survey 2018' (*European Commission*, 2018) <https://ec.europa.eu/info/sites/info/files/2017-comm-690_en_0.pdf> accessed 28 June 2018.

European Commission, 'Blue Book 2016: EU-Indonesia Development Cooperation In 2015 - International Cooperation and Development - European Commission' (*International Cooperation and Development*, 2017) <http://ec.europa.eu/europeaid/blue-book-2016-eu-indonesia-development-cooperation-2015_en> accessed 16 February 2017.

European Commission, 'Cloud computing Strategy - Digital Single Market - European Commission' (*EU Commission*, 2016) <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy> accessed 20 July 2016.

European Commission, 'Europe 2020 Strategy' (*European Commission*, 2018) <https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_en> accessed 28 June 2018.

European Commission, European Egovernment Action Plan 2016-2020 - Digital Single Market - European Commission' (*European Commission*, 2016) <https://ec.europa.eu/digital-single-market/en/node/81744> accessed 20 July 2016.

European Commission, 'European Employment Strategy - Employment, Social Affairs & Inclusion - European Commission' (*European Commission*, 2018) <http://ec.europa.eu/social/main.jsp?catId=101&intPageId=3427> accessed 28 June 2018.

European Commission, 'European Semester Thematic Factsheet - Active Labour Market Policies' (*Ec.europa.eu*, 2018) <https://ec.europa.eu/info/sites/info/files/file_import/european-semester_thematic-factsheet_active-labour-market-policies_en.pdf> accessed 20 January 2018.

European Commission, Press Release - Unleashing the Potential ofcloud computingin Europe - What Is It and What Does It Mean For Me?' (*Europa.eu*, 2012) <http://europa.eu/rapid/press-release_MEMO-12-713_en.htm> accessed 23 July 2016.

European Commission,'Results of the Public Consultation on the Europe 2020 Strategy' (Europa.eu, 2014) <http://ec.europa.eu/europe2020/pdf/europe2020stocktaking_en.pdf> accessed 5 October 2015.

European Commission, ‘Setting the Priorities’ (*European Commission*, 2018) <https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/european-semester-timeline/setting-priorities_en> accessed 28 June 2018.

European Commission,‘Skills Mismatches and Labour Mobility’ (EU) <http://ec.europa.eu/europe2020/pdf/themes/27_skills_gaps_and_labour_mobility.pdf > accessed 10 October 2016.

European Commission, ‘The Autumn Package Explained’ (*European Commission*, 2018) <https://ec.europa.eu/info/sites/info/files/the-autumn-package-explained_en.pdf> accessed 28 June 2018.

European Commission, ‘Taking Stock of The Europe 2020 Strategy for Smart, Sustainable and Inclusive Growth, COM(2014) 130 Final/2’ (Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, 2014) <http://ec.europa.eu/europe2020/pdf/europe2020stocktaking_en.pdf> accessed 11 October 2015.

European Commission, ‘Tasks of the Article 29 DPWP’ (*EU*, 2017) <http://ec.europa.eu/justice/data-protection/article-29/files/tasks-art-29_en.pdf> accessed 13 March 2017.

European Commission, Unleashing the Potential ofcloud computing in Europe [Interactive] (Brussels 2012).

European Commission, ‘Who We Are - Digital Single Market - European Commission’ (*European Commission*, 2016) <https://ec.europa.eu/digital-single-market/en/who-we-are-dg-connect> accessed 20 July 2016.

European Council, ‘A Renewed EU Strategy 2011-14 for Corporate Social Responsibility, COM(2011) 681 Final’ (Communication from The Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, 2011) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0681:FIN:en:PDF> accessed 11 October 2015.

European Telecommunications Standards Institute,‘The cloud Standards Coordination Final Report’ (*European Telecommunications Standards Institute*, 2013) <http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF> accessed 20 July 2016.

‘Executive Summary, Indonesia ICT Market Landscape Study’ (*International Data Corporation*) <http://mdecstaging.s3.amazonaws.com/2016/11/29/15/35/11/63cf68f4-f915-4831-99b9-f541a387300a/INDO-MDEC-Executive-Summary-vF3.pdf> accessed 21 February 2017.

Filippi P and Belli L, ‘Law of the cloud V Law of the Land: Challenges and Opportunities for Innovation’ (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/156/249> accessed 5 October 2015.

Filippi P and McCarthy S, ‘Cloud computing: Centralisation and Data Sovereignty’ (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/101/245> accessed 5 October 2015.

Fimin M, ‘Five Steps to Protect Confidential Data When Employees Leave’ (2017) 2017 Computer Fraud & Security.

Flick U, *Designing Qualitative Research* (1st edn, Sage Publications 2008).

Flick U, *Introducing Research Methodology* (1st edn, SAGE 2011).

Gandi F, ‘Cloud computing Set to Dominate Corporate Internet Services’ (The Jakarta Post, 2014) <http://www.thejakartapost.com/news/2014/04/29/the cloud-computing-set-dominate-corporate-internet-services.html> accessed 28 October 2015.

Gentile F, ‘ICT in Indonesia » Www.Ubibusiness.Com’ (Ubibusiness.com, 2014) <http://www.ubibusiness.com/topics/regulations/ict-in-indonesia/#.VhIHUZdfeJ> accessed 5 October 2014.

Gleeson N and Walden I, ‘It’s A Jungle Out There’?cloud computing, Standards and the Law’ (2014) 5 European Journal of Law and Technology <http://ejlt.org/article/view/363/461> accessed 5 October 2015.

Gomm R, *Social Research Methodology* (1st edn, Palgrave Macmillan 2008).

Gong C and others, ‘The Characteristics ofcloud computing’ [2010] 2010 39th International Conference on Parallel Processing Workshops.

Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M. and Pourzandi, M, ‘A Quantitative Analysis of Current Security Concerns and Solutions forcloud computing’ (2012) 1 Journal ofcloud computing: Advances, Systems and Applications.

Goyal S, ‘Public Vs Private Vs Hybrid Vs Community -cloud computing: A Critical Review’ (2014) 6 International Journal of Computer Network and Information Security.

Greenberg, A., Hamilton, J., Maltz, D. A. and Patel, P, ‘The Cost of a The cloud’ (2008) 39 ACM SIGCOMM Computer Communication Review.

Greenleaf G, 'The Influence Of European Data Privacy Standards Outside Europe: Implications For Globalization Of Convention 108' (2012) 2 International Data Privacy Law

Guilloteau S and Mauree V, ‘Privacy incloud computing’ (ITU-T Technology Watch Report, 2012) <https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf> accessed 10 October 2015.

Guruprasad, P. ‘A Study oncloud computingin Aviation and Aerospace’ (2015) 6 International Journal of Computer Science & Engineering Technology (IJCSET).

Habib, S., Hauke, S., Ries, S. and Mühlhäuser, M, ‘Trust as a Facilitator incloud computing: A Survey’ (2012) 1 Journal ofcloud computing: Advances, Systems and Applications.

Hailu A, ‘Factors Influencing The cloud-Computing Technology Adoption in Developing Countries’ (PhD, Capella University 2012).

Hanaysha J, ‘Examining the Effects of Employee Empowerment, Teamwork, And Employee Training on Organisational Commitment’ (2016) 229 Procedia - Social and Behavioural Sciences.

Handbook On European Data Protection Law (European Union Agency for Fundamental Rights and Council of Europe 2018)

Hashizume, K., Rosado, D. G., Fernández-Medina, E. and Fernandez, E. B, 'An Analysis of Security Issues forCloud Computing' (2013) 4 Journal of Internet Services and Applications.

Hassan K, 'Personal Data Protection in Employment: New Legal Challenges for Malaysia' (2012) 28 Computer Law & Security Review.

Hennink M, Hutter I and Bailey A, *Qualitative Research Methods* (1st edn, Sage 2011).

Hermana B and Silfianti W, 'Evaluating E-Government Implementation by Local Government: Digital Divide in Internet Based Public Services in Indonesia' (2011) 2 International Journal of Business and Social Science < http://www.ijbssnet.com/journals/Vol._2_No._3_[Special_Issue_-_January_2011]/18.pdf> accessed 5 October 2015.

Hill, R., Hirsch, L., Lake, P. and Moshiri, S, *Guide tocloud computing* (1st edn, Springer London 2012).

'History of ID-SIRTII/CC' (*Idsirtii.or.id*) <http://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html> accessed 3 February 2017.

Hu, P., Ning, H., Qiu, T., Xu, Y., Luo, X. and Sangaiah, A. K, 'A Unified Face Identification and Resolution Scheme Usingcloud computingin Internet of Things' (2018) 81 Future Generation Computer Systems.

Hugos M and Hulitzky D, *Business in thecloud* (1st edn, Wiley 2011).

Humphreys E, *Implementing ISO/IEC 27001 Isms Standard, Second Edition* (Artech House 2016).

Hussain, R., Son, J., Eun, H., Kim, S. and Oh, H, 'Rethinking Vehicular Communications: Merging VANET withcloud computing' [2012] 4th IEEE International Conference onCloud Computing Technology and Science Proceedings.

Hussain, S. A., Fatima, M., Saeed, A., Raza, I. and Shahzad, R. K, 'Multilevel Classification of Security Concerns incloud computing' (2017) 13 Applied Computing and Informatics.

Hwang IO Cha, 'Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance' (2018) 81 Computers in Human Behavior.

ICO, 'Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are' (*Information Commissioner's Office*, 2014) <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> accessed 19 July 2016.

ICO, 'Guide to Data Protection' (Ico.org.uk, 2016) <https://ico.org.uk/for-organisations/guide-to-data-protection/> accessed 18 July 2016.

Idowu S and Leal Filho W, *Professionals' Perspectives of Corporate Social Responsibility* (Springer 2009).

Igbaria M and Tan M, 'The Consequences of Information Technology Acceptance on Subsequent Individual Performance' (1997) 32 Information &Management .

Indonesia Central Bureau of Statistics, 'Percentage of Population Aged 7-24 Years by

Sex, School Age Group, And School Participation 1, 2002-2014' (Indonesia Central Bureau of Statistics 2015).

'Indonesia Growth Opportunity and Market Expansion' (*Eibn.org*) <http://eibn.org/> accessed 21 March 2018.

Inmor SR Suwannahong, 'The Acceptance ofcloud computingfor IT Workers in Thailand' (2017) 121 Procedia Computer Science.

Jaatun, M., Zhao, G., Vasilakos, A. V., Nyre, Å. A., Alapnes, S. and Tang, Y, 'The Design of a Redundant Array of Independent Net-Storages for Improved Confidentiality incloud computing' (2012) 1 Journal ofcloud computing: Advances, Systems and Applications.

Jaatun M, Lambrinoudakis C and Rong C, 'Special Issue on Security incloud computing' (2012) 1 Journal ofcloud computing: Advances, Systems and Applications.

Jadeja Y and Modi K, 'Cloud computing - Concepts, Architecture and Challenges' [2012] 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET).

Jain A, Kumar M and Lambha A, 'An Overview and Trends incloud computing' [2015] International Journal of Computer Applications.

Jakimoski K, 'Security Techniques for Data Protection incloud computing' (2016) 9 International Journal of Grid and Distributed Computing <http://dx.doi.org/10.14257/ij gdc.2016.9.1.05> accessed 4 November 2016.

Janal D, *Risky Business* (1st edn, Toronto 1998).

Janssen MN Helbig, 'Innovating and Changing the Policy-Cycle: Policy makers Be Prepared!' [2016] Government Information Quarterly.

Jiang Y, 'Managerial Incentives in The Presence of Golden Handshakes' (2017) 20 Finance Research Letters.

Johnson W, 'Managing University Technology Development Using Organisational Control Theory' (2011) 40 Research Policy.

Jonker J and Pennink B, *The Essence of Research Methodology* (1st edn, Springer 2010).

Jung J, 'Technology, Skill, And Growth in A Global Economy' (Econpapers.repec.org, 2015) <http://EconPapers.repec.org/RePEc:ema:worpap:2015-08> accessed 5 October 2015.

Kaaniche NM Laurent, 'Data Security and Privacy Preservation inThe cloud Storage Environments Based on Cryptographic Mechanisms' (2017) 111 Computer Communications.

Kaplan R and Norton D, *the Strategy-Focused Organisation* (Harvard Business School Press 2001).

Kapurubandara M and Lawson R, 'Barriers to Adopting ICT and E-Commerce with SMEs in *Developing Countries: An Exploratory Study in Sri Lanka', Collaborative Electronic Commerce Technology and Research* (Collector Group 2006).

Kaufman L, 'Data Security in the World ofcloud computing' (2009) 7 IEEE Security & Privacy Magazine.

Kemp R, ‘Legal Aspects of The cloud Security’ (2018) 34 Computer Law & Security Review.

'Kevin Bunsell' (*Ico.org.uk*, 2019) <https://ico.org.uk/action-weve-taken/enforcement/kevin-bunsell/> accessed 11 April 2019

Kim S, ‘Managing Millennials’ Personal Use of Technology at Work’ (2018) 61 Business Horisons.

Kizza J, *Guide to Computer Network Security* (Springer 2015).

Koutinas, A. A., Sypsas, V., Kandylis, P., Michelis, A., Bekatorou, A., Kourkoutas, Y., Kordulis, C., Lycourghiotis, A., Banat, I. M., Nigam, P., Marchant, R., Giannouli, M. and Yianoulis, P, ‘Nano-Tubular Cellulose for Bioprocess Technology Development’ (2012) 7 PLoS ONE.

Kumar P, P RajPJelciana, ‘Exploring Data Security Issues and Solutions incloud computing’ (2018) 125 Procedia Computer Science.

Kumar R, *Research Methodology* (1st edn, Sage 2009).

Kumara A, S BhatiabIChianga, ‘Deployment of An In-House Designed Training Process in A Quaternary Care Hospital’ (2013) 21 Technology and health care: official journal of the European Society for Engineering and Medicine.

‘Laporan Tahunan Kementerian Komunikasi Dan InformatikaTahun 2016’ (*web.kominfo.go.id*, 2018) <https://web.kominfo.go.id/sites/default/files/users/12/LAPORAN%20TAHUNAN%20KOMINFO%202016.pdf> accessed 2 July 2018.

Lei, Z., Zhang, B., Zhang, W., Li, Q., Zhang, X. and Peng, J, ‘Comparison of Severalcloud computing Platforms’, *Second International Symposium on Information Science and Engineering* (2009).

Leimbach, T., Hallinan, D., Bachlechner, D., Weber, A., Jaglo, M., Hennen, L., Nielsen, R. Ø., Nentwich, M., Strauss, S., Lynn, T. and Hunt, G, ‘Potential and Impacts ofcloud computing Services and Social Network Websites’ (European Parliamentary Research Service, 2016) <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf> accessed 9 July 2016.

Leimeister, S., Böhm, M., Riedl, C. and Krcmar, H, ‘The Business Perspective ofcloud computing: Actors, Roles and Value Networks’, *18th European Conference on Information Systems* (ECIS 2010 Proceedings 2010) <http://aisel.aisnet.org/ecis2010/56> accessed 14 February 2017.

Lenk, A., Klems, M., Nimis, J., Tai, S. and Sandholm, T, ‘What’s Inside the cloud? An Architectural Map of the cloud Landscape’ [2009] 2009 ICSE Workshop on Software Engineering Challenges ofcloud computing.

Levitin G, L XingY Dai, ‘Co-Residence Based Data Vulnerability Vs. Security incloud computing System with Random Server Assignment’ (2018) 267 European Journal of Operational Research.

Lim V, ‘The IT Way of Loafing on the Job: Cyberloafing, Neutralising and Organisational Justice’ (2002) 23 Journal of Organisational Behavior.

Liu, S., Chan, F. T., Yang, J. and Niu, B, ‘Understanding the Effect ofcloud computing on Organisational Agility: An Empirical Examination’ (2018) 43

International Journal of Information Management.

Liu, Q., Srinivasan, A., Hu, J. and Wang, G, 'Preface: Security and Privacy in Big Data The clouds' (2017) 72 Future Generation Computer Systems.

Lloyd I, 'From Ugly Duckling to Swan. The Rise of Data Protection and Its Limits' (2018) 34 Computer Law & Security Review.

Maclean R and Jagannathan S, *Skills Development for Inclusive and Sustainable Growth in Developing Asia-Pacific* (Springer 2013).

Madalina O, 'Conflict Management, A New Challenge' (2016) 39 Procedia Economics and Finance.

Mangula I, van de Weerd I and Brinkkemper S, 'Adoption ofThe cloud Business Model in Indonesia' [2012] Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services - IIWAS '12.

Marchini R,*Cloud Computing*(BSI 2010).

Marentette K, Johnson A and Mills L, 'A Measure of Cross-Training Benefit Versus Job Skill Specialisation' (2009) 57 Computers & Industrial Engineering.

Marinescu D,Cloud Computing*: Theory and Practice* (1st edn, Morgan Kaufmann Publishers 2013).

Marler J, 'Training and Effective Employee Information Technology Use' (2006) 32 Journal of Management.

Marsh A, *Employee Relations Policy and Decision Making* (Gower 1982).

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A, 'Cloud Computing– The Business Perspective' (2011) 51 Decision Support Systems.

Maruyama G and Ryan C, *Research Methods in Social Relations* (1st edn, John Wiley & Sons 2014).

McConville M and Chui W, *Research Methods for Law* (1st edn, Edinburgh University Press 2007).

McCullagh K, 'Response to EU Commission Public Consultation oncloud computing' (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/137/228> accessed 22 July 2016.

McKinsey&Company, 'Ten Ideas to Maximise the Socioeconomic Impact of ICT in Indonesia' (2015).

McNeill P and Chapman S, *Research Methods* (1st edn, Routledge 2005).

Medudula M, M Sagar, R Gandhi, 'Telecom Players, Regulatory Bodies, International Organisations and Regional Telecom Statistics: Global Overview' [2016] Telecom Management in Emerging Economies.

'Measuring the Information Society Report 2016' (*International Telecommunication Union*) <http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf> accessed 21 February 2017.

Mendonça J and others, 'Disaster Recovery Solutions For IT Systems: A Systematic Mapping Study' (2019) 149 Journal of Systems and Software

‘Methodology Dictionary Definition | Methodology Defined’ (Yourdictionary.com) <http://www.yourdictionary.com/methodology#websters> accessed 26 August 2015.

Milligan C, Biggs H and Bishop L, ‘Meeting the Requirements of the Data Protection Act (1998)’ (Faculty of Health and Medicine (Division of Health Research), Lancaster University) <https://www.lancaster.ac.uk/researchethics/1-7-dataproact.html> accessed 13 March 2015.

Millard C,*Cloud Computing Law* (Oxford University Press 2013).

Millard, W.C. ‘Banking inThe cloud: Part 2 – Regulation ofThe cloud As ‘Outsourcing’ (2018) 34 Computer Law & Security Review.

Ministry of Communication and Information Technology Republic of Indonesia, ‘ICT Research and Development in Indonesia’ (*Ministry of Communication and Information Technology Republic of Indonesia*, 2015) <https://www.nict.go.jp/en/asean_ivo/4otfsk00001ver81-att/a1436766621134.pdf> accessed 22 February 2016.

Mitić, S., Nikolić, M., Jankov, J., Vukonjanski, J. and Terek, E, ‘The Impact of Information Technologies on Communication Satisfaction and Organisational Learning in Companies in Serbia’ (2017) 76 Computers in Human Behavior.

Mohammed B and others, 'Failure Analysis Modelling In An Infrastructure As A Service (Iaas) Environment' (2018) 340 Electronic Notes in Theoretical Computer Science

Mohamed E, Abdelkader H and EI-Etriby S, ‘Enhanced Data Security Model forcloud computing’, *the 8th International Conference on INFOrmatics and Systems* (2012).

Monteleone S, ‘Privacy and Data Protection at the Time of Facial Recognition: Towards a New Right to Digital Identity?’ (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/168/257> accessed 5 May 2016.

Mantelero A, ‘Cloud computing, Trans-Border Data Flows and the European Directive 95/46/EC: Applicable Law and Task Distribution’ (2012) 3 European Journal of Law and Technology <http://ejlt.org/article/view/96/254> accessed 5 October 2015.

Morris C and Murphy C, *Getting a PhD in Law* (Hart Pub 2011).

National Institute of Standards and Technology, ‘The NIST Definition ofcloud computing’ (Computer Security Division, National Institute of Standards and Technology 2011).

Newby T, *Validating Your Training* (Kogan Page 1992).

Ngo F and Paternoster R, ‘Cybercrime Victimisation: An Examination of Individual and Situational Level Factors’ (2011) 5 International Journal of Cyber Criminology.

Noor, T. H., Zeadally, S., Alfazi, A. and Sheng, Q. Z, ‘Mobilecloud computing: Challenges and Future Research Directions’ (2018) 115 Journal of Network and Computer Applications.

Nyikes Z, ‘Digital Competence and The Safety Understanding Base on The Assessments Results of The Middle East-European Generations’ (2018) 22 Procedia Manufacturing.

Nykodym N, Ariss S and Kurtz K, ‘Computer Addiction and Cyber Crime’ [2008]

Journal of Leadership, Accountability and Ethics.

OECD, OECD Guidelines for Multinational Enterprises, 2011 Edition (OECD Publishing 2011).

OLD, 'Research_1 Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced Learner's Dictionary at Oxfordlearnersdictionaries.Com' (Oxfordlearnersdictionaries.com) <http://www.oxfordlearnersdictionaries.com/definition/english/research_1?q=research > accessed 4 October 2015.

Ooi, K., Lee, V., Tan, G. W., Hew, T. and Hew, J, 'Cloud computingin Manufacturing: The Next Industrial Revolution in Malaysia?' (2018) 93 Expert Systems with Applications.

Oppenheim C, the No-Nonsense Guide to Legal Issues in Web 2.0 Andcloud computing (1st edn, Facet 2012).

Oxford English Dictionary - Research, N.1' (*Oed.com*, 2017) <http://www.oed.com/view/Entry/163432?rskey=RPJnyl&result=1&isAdvanced=false#eid> accessed 26 August 2015.

Pantea S, A SabadashFBiagi, 'Are ICT Displacing Workers in The Short Run? Evidence from Seven European Countries' (2017) 39 Information Economics and Policy.

Parasol M, 'The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, And on China's Big Data and Smart City Dreams' (2018) 34 Computer Law & Security Review.

Pattinson C, 'ICT And Green Sustainability Research and Teaching' (2017) 50 IFAC-PapersOnLine.

Peace A, Galletta D and Thong J, 'Software Piracy: A Model and Empirical Test' (2003) 20 Journal of Management Information Systems.

Perrons RA Hems, 'Cloud computing in The Upstream Oil & Gas Industry: A Proposed Way Forward' (2013) 56 Energy Policy.

Phillips, J. C., Hargons, C., Chung, Y. B., Forrest, L., Hahn Oh, K. and Westefeld, J, 'Society ofCounseling Psychology Leadership Academy: Cultivating Leadership Competence and Community' (2017) 45 The Counseling Psychologist.

Pitman T, 'Training Success' (2014) 37 Business and Economics--Banking and Finance.

'Proposal for A Council Decision on Guidelines for The Employment Policies of The Member States' (*European Commission*, 2018) <https://ec.europa.eu/info/sites/info/files/2017-comm-677_en.pdf> accessed 28 June 2018.

PT. Telekomunikasi Indonesia, 'Annual Report 2012' (PT. Telekomunikasi Indonesia, Tbk., 2012) <http://www.telkom.co.id/download/File/UHI/2013/AR2012/TelkomAR2012.pdf> accessed 18 November 2014.

PT. Telekomunikasi Indonesia, 'Annual Report 2015' (*PT Telekomunikasi Indonesia, Tbk*, 2015) <http://www.telkom.co.id/assets/uploads/2013/05/AR-TELKOM-2015_ENG.1.pdf> accessed 3 October 2016.

PT. Telekomunikasi Indonesia,Annual Report 2016 (PT Telekomunikasi Indonesia, Tbk 2017) <https://konten.telkom.co.id/cs/groups/cem/documents/document/wcc009290.pdf> accessed 24 February 2018.

PT. Telekomunikasi Indonesia 'Annual Report 2016' (*Telkomsel.com*, 2017) <https://www.telkomsel.com/en/about-us> accessed 28 August 2017.

Purnomo S and Lee Y, 'An Assessment of Readiness and Barriers towards ICT Programme Implementation: Perceptions of Agricultural Extension Officers in Indonesia' (2010) 6 International Journal of Education and Development using Information and Communication Technology <http://files.eric.ed.gov/fulltext/EJ1085021.pdf> accessed 17 November 2017.

Provos N, Rajab M and Mavrommatis P, 'Cybercrime 2.0' (2009) 52 Communications of the ACM.

Rae L, *How to Measure Training Effectiveness* (3rd edn, Gower 1997).

Ramachandra G, M IftikharF Khan, 'A Comprehensive Survey on Security incloud computing' (2017) 110 Procedia Computer Science.

Reese G, *Cloud Application Architectures* (O'Reilly 2009).

Riccucci N, *Public Personnel Management* (5th edn, 2015).

Riszuto T, 'Age and Technology Innovation: Does Work Context Matter?' (2011) 27 Computers in Human Behavior.

Robinson N, *TheCloud* (1st edn, Rand 2011).

Rokhman A, 'E-Government Adoption in Developing Countries; The Case of Indonesia' (2011) 2 Journal of Emerging Trends in Computing and Information Sciences <http://www.cisjournal.org/archive/vol2no5/vol2no5_4.pdf> accessed 5 October 2015.

Ryan M, 'Cloud computing Privacy Concerns on Our Doorstep' (2011) 54 Communications of the ACM.

SamGnanakkan S, 'Mediating Role of Organisational Commitment on HR Practices and Turnover Intention among ICT Professionals' (2010) 10 Journal of Management Research.

Schultze UM Avital, 'Designing Interviews To Generate Rich Data For Information Systems Research' (2011) 21 Information and Organization.

Schwab K, The Global Competitiveness Report 2013-2014 (World Economic Forum 2013).

Scott, C.P. 'Employment, Technology and Industrial Relations in The UK Clearing Banks: Is the Honeymoon Over?' (1992) 7 New Technology, Work and Employment.

Segura-Serrano A, 'Cybersecurity: Protection of Critical Information Infrastructures and Operators' Obligations' (2015) 6 European Journal of Law and Technology <http://ejlt.org/article/view/396/592> accessed 5 June 2016.

Selvamani, R. 'Data Security Challenges and Its Solutions incloud computing' (2015) 48 Procedia Computer Science.

Shaikh RM Sasikumar, 'Data Classification for Achieving Security inCloud

Computing' (2015) 45 Procedia Computer Science.

'Shamim Sadiq' (*Ico.org.uk*, 2019) <https://ico.org.uk/action-weve-taken/enforcement/shamim-sadiq/> accessed 11 April 2019

Siburian H, 'Emerging Issue in Cyber Crime: Case Study Cyber Crime in Indonesia' (2016) 5 International Journal of Science and Research (IJSR).

Simmonds M, 'Instilling A Culture of Data Security Throughout the Organisation' (2018) 2018 Network Security.

Singh AK Chatterjee, 'The cloud Security Issues and Challenges: A Survey' (2017) 79 Journal of Network and Computer Applications.

Singh S, Y JeongJ Park, 'A Survey oncloud computing Security: Issues, Threats, And Solutions' (2016) 75 Journal of Network and Computer Applications.

Snieder R and Larner K, *The Art of Being A Scientist* (1st edn, Cambridge University 2010).

Smith P, 'Learners and Their Workplaces: Towards A Strategic Model of Flexible Delivery of Training' (2001) 53 Journal of Vocational Education & Training.

Soliman F, 'Modelling the Appraisal of The Cloud Systems' Implementation' (2012) 8 Journal of Modern Accounting and Auditing.

Stanoevska-Slabeva K, Wozniak T and Ristol S, *Grid andcloud computing* (Springer 2010).

Steenhuis H and De Bruijn E, 'High Technology Revisited: Definition and Position' (2006) 2 2006 IEEE International Conference on Management of Innovation and Technology <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4037187> accessed 28 July 2016.

Stergiou, C., Psannis, K. E., Kim, B. and Gupta, B, 'Secure Integration of IoTAndcloud computing' (2018) 78 Future Generation Computer Systems.

Stimel DL Sekerka, 'Play Fair! Innovating Internal Self-Regulation in The Market for Profit' (2018) 61 Business Horizons.

Stitilis D and Malinauskaite I, 'Compliance with Basic Principles of Data Protection in Cloud Computing: The Aspect of Contractual Relations with End-Users' (2014) 5 European Journal of Law and Technology <http://ejlt.org/article/view/231/422> accessed 5 August 2016.

Stylianou K, Venturini J and Zingales N, 'Protecting User Privacy in the cloud: An Analysis of Terms of Service' (2015) 6 European Journal of Law and Technology <http://ejlt.org/article/view/462/594> accessed 5 August 2016.

Subashini S and Kavitha V, 'A Survey on Security Issues in Service Delivery Models ofcloud computing' (2011) 34 Journal of Network and Computer Applications.

Subramanian NA Jeyaraj, 'Recent Security Challenges incloud computing' (2018) 71 Computers & Electrical Engineering.

Sukumaran SM Mohammed, 'PCR And Bio-Signature for Data Confidentiality and Integrity in Mobilecloud computing' [2018] Journal of King Saud University - Computer and Information Sciences.

Sullivan J, *Creating Employee Champions*(DoSustainability 2014).

Surendro K and Fardani A, ‘Identification of SME Readiness to Implementcloud computing’ [2012] 2012 International Conference oncloud computing and Social Networking (ICCCSN).

Tarafdar M, Gupta A and Turel O, ‘The Dark Side of Information Technology Use’ (2013) 23 Information Systems Journal.

Tari Z and others, ‘Security and Privacy inCloud Computing: Vision, Trends, and Challenges’ (2015) 2 IEEE CloudComput.

Tas E, ‘ICT Education for Development – A Case Study’ (2011) 3 Procedia Computer Science.

Telkom, ‘Code of Ethics and Corporate Culture’ (*Telkom.co.id*, 2018) <https://www.telkom.co.id/servlet/tk/mobile/about/en_US/stockdetail/code-of-ethics-and-corporate-culture.html> accessed 29 June 2018.

Telkom, ‘Telkom Group Organisation Structure’ (*Telkom.co.id*, 2018) <https://www.telkom.co.id/servlet/tk/mobile/about/en_US/companystructure/telkom-group-en.html> accessed 26 June 2018.

'Telkom Corporate University Learning Journey' (Telkom Corporate University 2017)

Telkomsigma, ‘About Us - Telkomsigma’ (*Telkomsigma*, 2017) <http://www.telkomsigma.co.id/about-us/> accessed 28 August 2017.

Telkomsigma, ‘Cloud computing Infrastructure Technology - Telkomsigma’ (Telkomsigma) <http://www.telkomsigma.co.id/cloud-computing/> accessed 22 January 2015.

Telkomsigma, ‘IT Consulting Services & System Integration - Telkomsigma’ (Telkomsigma) <http://www.telkomsigma.co.id/it-consulting-services-system-integration/> accessed 10 October 2016.

Teneyuca D, ‘Internet Cloud Security: The Illusion of Inclusion’ (2011) 16 Information Security Technical Report.

‘The 2016 Survey of Penetration and Behaviour of Indonesia’s Internet User’ (*Apjii.or.id*, 2017) <http://www.apjii.or.id/survei2016> accessed 3 February 2017.

Thompson PJ Chen, ‘Disagreements, Employee Spinoffs and The Choice of Technology’ (2011) 14 Review of Economic Dynamics.

Tikkinen-Piri C, A RohunenJ Markkula, ‘EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies’ (2018) 34 Computer Law & Security Review.

Toosi, A. N., Vanmechelen, K., Ramamohanarao, K. and Buyya, R, ‘Revenue Maximisation with Optimal Capacity Control in Infrastructure as a Service The cloud Markets’ (2015) 3 IEEE Transactions oncloud computing.

Thuraisingham B, *A Comprehensive Overview Of Secure Cloud Computing*(2012).

Townsend A and Bennett J, ‘Information Technology and Employment Law: Challenges in an Evolving Workplace’ (2003) 24 Journal of Labour Research.

Turnbull, L., Ochieng, H., Kadlec, C. and Shropshire, J, ‘Improving Service Continuity: IT Disaster Prevention and Mitigation for Data Centres’ [2013] Proceedings of the 2nd annual conference on Research in information technology - RIIT ‘13.

Uciu, G., Fratu, O., Halunga, S., Cernat, C. G., Poenaru, V. and Suciu, V, 'Cloud Consulting: ERP and Communication Application Integration in Open Source Cloud Systems' [2011] 2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers.

Ugur MA Mitra, 'Technology Adoption and Employment in Less Developed Countries: A Mixed-Method Systematic Review' (2017) 96 World Development.

Vafamehr AM Khodayar, 'Energy-AwareCloud Computing' (2018) 31 The Electricity Journal.

van de Weerd I, I MangulaSBrinkkemper, 'Adoption of Software as A Service in Indonesia: Examining the Influence of Organisational Factors' (2016) 53 Information & Management.

van Dijk M and Szirmai A, 'Industrial Policy and Technology Diffusion: Evidence from Paper Making Machinery in Indonesia' (2006) 34 World Development.

Vaquero, L. M., Rodero-Merino, L., Caceres, J. and Lindner, M, 'A Break in theClouds' (2008) 39 ACM SIGCOMM Computer Communication Review.

Varghese BR Buyya, 'Next GenerationCloud Computing: New Trends and Research Directions' (2018) 79 Future Generation Computer Systems.

Vergouw, C.B. 'Promising Policing Technologies: Experiences, Obstacles and Police Needs Regarding Law Enforcement Technologies' (2015) 31 Computer Law & Security Review.

Vogelsang I, 'Regulatory Inertia Versus ICT Dynamics: The Case of Product Innovations' (2017) 41 Telecommunications Policy.

'Vote Leave Limited' (*Ico.org.uk*, 2019) <https://ico.org.uk/action-weve-taken/enforcement/vote-leave-limited/> accessed 11 April 2019

Vouk M, 'Cloud computing: Issues, Research and Implementations' (2008) 16 Journal of Computing and Information Technology.

Walden I and Angel J, *Telecommunications Law and Regulation* (Oxford University Press 2005).

Walter D, 'Competency-Based On-The-Job Training for Aviation Maintenance and Inspection – A Human Factors Approach' (2000) 26 International Journal of Industrial Ergonomics.

Wang L, *Cloud Computing*(1st edn, CRC Press 2012).

Wang R, 'Research on Data Security Technology Based in Cloud Storage' (2017) 174 Procedia Engineering.

Wardhaugh B, 'Developing Regimes and Mobile Telecoms Regulation in the Twenty-First Century: Who Makes the Call?' (2015) 6 European Journal of Law and Technology (EJLT) <http://ejlt.org/article/view/402/579> accessed 8 June 2016.

Warren A, 'Fully Compliant? A Study of Data Protection Policy In UK Public Organisations' (Ph D, Loughborough University 2003)

Watkins D and Burton M, *Research Methods in Law* (1st edn, Routledge 2013).

Watson P, 'a Multi-Level Security Model for Partitioning Workflows over Federated Clouds' (2012) 1 Journal ofCloud Computing: Advances, Systems and Applications.

Weinhardt C and others, ‘Cloud Computing – A Classification, Business Models, And Research Directions’ (2009) 1 Business & Information Systems Engineering.

Weinman J, ‘The Strategic Value of the Cloud’ (2015) 2 IEEECloud Computing.

Wicks, P., Stamford, J., Grootenhuis, M. A., Haverman, L. and Ahmed, S, ‘Innovations in E-Health’ (2013) 23 Quality of Life Research.

Wijaya, A. A., Purnama, J., Amin Soetomo, M. A. and Eng, K. I, ‘Indonesian Awareness of Health Record Stored incloud computing’ [2014] 2014 International Conference on ICT for Smart Society (ICISS).

Williams A, *Publiccloud computing* (1st edn, Nova Science Publishers 2012).

Williams R, ‘The Lantern-Bearers of the History of Technology’ (2013) 29 History and Technology.

Wood, T., Cecchet, E., Ramakrishnan, K., Shenoy, P., Van Der Merwe, J. and Venkataramani, A, ‘Disaster Recovery as a The cloud Service: Economic Benefits & Deployment Challenges’, *2nd USENIX conference on hot topics incloud computing* (USENIX 2010).

Wu, Z., Tian, L., Li, P., Wu, T., Jiang, M. and Wu, C, ‘Generating Stable Biometric Keys for Flexiblecloud computing Authentication Using Finger Vein’ (2018) 433-434 Information Sciences.

Xu X, ‘Fromcloud computingtoThe cloud Manufacturing’ (2012) 28 Robotics and Computer-Integrated Manufacturing.

Yallop C, Macquarie Dictionary (Macquarie Library 2005).

Yoo C, G SandersRCerveny, ‘Exploring the Influence of Flow and Psychological Ownership on Security Education, Training andUnderstanding Effectiveness and Security Compliance’ [2018] Decision Support Systems.

Yu W and Ramanathan R, ‘Business Environment, Employee Competencies and Operations Strategy: An Empirical Study of Retail Firms in China’ (2012) 24 IMA Journal of Management Mathematics.

Zanella R and Blount S, *Cloud Security and Governance: Who’s on Your Cloud?* (1st edn, IT Governance Ltd 2010).

Zhang Q, Cheng L and Boutaba R, ‘Cloud Computing: State-Of-The-Art and Research Challenges’ (2010) 1 Journal of Internet Services and Applications .

Zhong, C., Lin, T., Liu, P., Yen, J. and Chen, K, ‘A Cyber Security Data Triage Operation Retrieval System’ (2018) 76 Computers & Security.

Appendices

Appendix 1 – Ethical consent form

Lancaster University

An Analysis of the legal and corporate responsibility framework relating to the growth of the Indonesian cloud computing industry.

As an employee of PT Telkom Indonesia, Tbk., I have gained a scholarship from PT Telkom Indonesia, Tbk., I am currently a Ph.D. student at the Law School at Lancaster University, UK. The objective of my research is to analyze the relevant Indonesian and UK law, policy and regulation to evaluate the relationship between the employer/employee relationship in the light of the growth of cloud computing.
Please read and consider the following information before deciding whether you would like to participate in the study.

What is this study about?
I would like to interview senior managements who have the authority to make company policy on the development of the legal and corporate responsibility framework relating to the growth of the Indonesian cloud computing industry. I am interested in participants' views on how decisions made. Their perception and motivation in the making of the decision/ policy, what influenced them in making the decision/ policy, and what were/ are their experiences related to the implementation of the decision/ policy.

Why have I been approached?
You have been identified by me as a researcher as a possible participant in this study because of your role as a senior management who has the authority to make company policy.

What will I be asked to do if I take part in this study?
You will be asked to agree to be interviewed by me. The interview may take up to an hour and will be held on a date, time and place to suit you. I anticipate that the interview will take place in a suitable room at your place of work, such as an office or meeting room.
Before the interview starts, you will be asked to read and sign a Consent Form. If you agree, the interview will be audio recorded and note taking. All interviews will be coded prior to transcription to ensure anonymity. Only I will know your identity. If you do not agree to be recorded, I will take notes during the interview and will code those note to ensure your anonymity.

What do I do if I would like to take part in this study?
If you would like to take part in this study, please contact me by email to Rama Kumala Sari (r.sari@lancaster.ac.uk)

Do I have to take part?
No. It is your choice whether to take part in this study. You are under no obligation to participate. There are no incentives for agreeing to take part, and there are no benefits to taking part. You do not need to offer an explanation if you decide not to take part.

Are there any risks to taking part in this study?

The interviewer is an employee of the company, and the company has funded this research. The company itself will have no access to the primary data, and all responses will be anonymised. Furthermore, the research is being carried out in an independent manner, and the company has no input into or control over the research process or the presentation of the findings.

Your position in the company will not be included, and direct quotations will not be used where there is the possibility of identifying the participant. The researcher will only pose questions on questioned the perspective of the interviewees in terms of making decisions related to the policy on employment in the company. The questions will only seek to determine what the interviewees' considerations are before making such policy in the company. No specific details will be requested. The questions of the interview questions will not be designed to disclose a confidential information of the company. You will be able to read the interview transcript after it has finished and request that any part or the interview in its entirety by destroyed. Due to these approaches no risks are anticipated if you participate in this study, but if you experience any distress during the interview, I will stop the interview and any recording. I will ask if you want to continue with the interview. If you do not want, I will contact you a week later to see if you want to resume the interview. Or whether you want the data collected in the part interview to be included in the study. If you do not, I will securely destroy that data.

The overarching aim of the research is to determine a policy that will support employees in the light of the growth of cloud computing. It will, therefore, give numbers of key policy makers within institutions a voice in determining future policy based on their experience. The research will be approached in a way that sees the researcher and the participants working together to predict future trends.

Withdrawal from the study

You can refuse to answer any question during the interview or stop it without offering any explanation. You can also withdraw from the study, without offering any explanation, up to three weeks after the interview has been conducted. If you stop your interview and or withdraw from the study, no data collected prior to stopping the interview or withdrawing from the study will be used without your permission.

Will my data be confidential?

Yes. The information you provide is confidential and will be anonymised when it is disseminated. Only the researcher will know the identity of the interviewee. The anonymization of the data will be randomised so that it will not be open to deduce who made which statements based upon the order of the interviews.

During and after the study, all data will be my responsibility and will be stored securely on University premises. Recordings of interviews will be deleted as soon as they have been transcribed, and the recordings and transcriptions will be transferred via an encrypted USB stick. Hard copies of transcriptions or notes of the interview will be kept in a locked filing cabinet on University premises in the researcher's supervisor's office. Electronic data files will be encrypted and stored on password protected University computers. All data will only accessible to the researcher. All data relating to the study will be securely destroyed ten years after the study has been completed.

If you are suspecting any malpractice on confidentiality during the study, you may send a caveat to the Director of Postgraduate Studies (Research), Law School, Lancaster University School of Law to discuss the suspected malpractice. Contact details are provided below.

Malpractice in the company
If you disclose information about malpractice in the company, your information will not be disclosed unless you agree that your statement can be disclosed. If serious malpractice is revealed that could potentially disclose criminal activities then I will approach the relevant authorities with this information.

Presentations of the findings
I will publish papers from the research, and the thesis will be made openly available. I may as well, present the findings to the company and the research participants. However, the presentations of the findings will only disclose the conclusions of the research. It will not reveal the identity of individual participants. Only the findings of the research will be presented to the company. These findings are related to the outcomes of the research which is a voice in determining future policy based on the policy makers' experiences in the company. As always, confidentiality will be maintained throughout, and all data will be anonymised.

Who has reviewed the study?
The study has been approved by Lancaster University's Research Ethics Committee.

Where can I obtain further information about the study?
If you have any questions please contact Rama Kumala Sari (r.sari@lancaster.ac.uk, +447743462966) – Law School, Lancaster University School of Law, Lancaster, LA1 4YN or my supervisor, **Dr Catherine Easton** (c.easton@lancaster.ac.uk, +441524592530) – Lecturer, Lancaster University School of Law, Bowland North, Lancaster, UK, LA1 4YN.

What if I have concerns about any aspects of the study?
If you do not want to speak to me or my supervisor or complaint relating to this study, please contact James Sweeney (j.sweeney@lancaster.ac.uk, +441524594263) – Director of Postgraduate Studies (Research), Law School, Lancaster University School of Law, Lancaster, LA1 4YN.

Thank you for reading this information sheet.

Rama Kumala Sari

Lancaster University

Consent Form

***PROJECT TITLE:** An Analysis of the legal and corporate responsibility framework relating to the growth of the Indonesian cloud computing industry.*

Name of Researcher: Rama Kumala Sari, Lancaster University, UK

Please initial box

1.	I have read and understand the Participant Information Sheet given to me for the above study, and have had the opportunity to ask questions.	☐
2.	I understand that my participation is voluntary and I am free to withdraw from this study, without giving any reasons, and that my legal rights will not be affected. I am free to refuse to answer any question.	☐
3.	I understand that if I want to withdraw from the study I can do so at any point up to three weeks after the interview has been conducted.	☐
4.	I understand that if I withdraw up to three weeks after my interview has been conducted, any data collected will not be used without my consent.	☐
5.	I understand that my interview will be recorded and transcribed by a professional transcriber external to the study, who will sign a Confidentiality Agreement, and will not know my identity.	☐
6.	I understand that anonymised quotes from my interview may be used in dissemination of the research, and that any personal data will remain confidential, and my details known only to the researchers.	☐
7.	I understand that the transcription or interviews notes will be kept in a locked filing cabinet on University premises. Any electronic files will be encrypted and stored on a password protected University computer. No-one other than the researchers will be able to access data collected for this study. All data will be securely destroyed 10 years after the study has been completed.	☐
8.	I agree to participate in this study.	☐
9.	I agree to my interview being audio-recorded.	☐
10.	I understand that any information given by me may be used in future reports, articles or presentations by the researcher	☐

Name of Participant (printed)	Participant's Signature	Date
Name of Researcher (printed)	Researcher's Signature	Date

When completed, please return to the researcher. One copy will be given to the participant and the original is to be kept in the file of the researcher.

Appendix 2 – Interview questions

An Analysis of the Legal and Employment Framework Related to the Growth of the Indonesian Cloud Computing Industry

Interview Agenda

Average interview time: 55-60 minutes

Interviewee:

Age:

Current position in the company:

Duration of the interviewee in the current position:

Date:

Time:

Introduction Thank you for your willingness to participate through interview in this project. My name is Rama Kumala Sari. I'm a PhD student in Lancaster University, UK. First of all, I would like you to take your time to read participant information sheet and sign the consent form to take part on this interview. I guarantee that your identity as well as your position in the company will be confidential and the result of this interview would not reveal your identity. I also would like to inquire your willingness to be recorded and I would take note during the interview to make sure the accuracy of your information. Should there be no more further question, I will explain the subject of this interview.

The overarching aim of the research is to determine a policy that will support employees in the light of the growth of cloud computing. It will, therefore, give a voice in determining future policy based on your experience. Focus of this project is the development of technology, especially in cloud computing. This project will analyze the Indonesian regulation and to look for the United Kingdom as well as Europan Union as comparation.

This interview will elaborate your view and background in making a policy in the company. This interview will seek your consideration in policy-making.

If you experience any distress during the interview, I will stop the interview and any recording. I will ask if you want to continue with the interview. If you do not want, I will contact you a week later to see if you want to resume the interview. Or whether you want the data collected in the part interview to be included in the study. If you do not, I will securely destroy that data.

If you agree with the term and condition, I will start the interview.

Stage		Question
Questions related to cloud and its implementation in the workplace;	Q1	Could you tell me your position in the company and how long have you been in that position? (This information will be anonymised; this information is intended to seek the relation between position and how the policy is being made)
	Q2	What are the main issues in practice related to the skills of employees to consider due to the growth of technology such as cloud computing?
	Q3	Can you explain the current approach to employee skills development in the light of the growth of technology such as cloud computing?
	Q4	Has the use of cloud computing transformed the behaviour of the employees in the company?
	Q5	What do you understand to be the rights of employees in the light of the growth of technology in the industry?
	Q6	Do you believe that developing employees' skills is a duty the company holds?
	Q7	Currently, what training is available for employees?
	Q8	Do you think that company should provide training for its employees related to the growth of technology?
	Q9	What kind of training or knowledge do you know of that is not currently provided by the company and that might be useful for employees in the light of the growth of technology?
	Q10	Do you know of any other ways for addressing the impact of the growth of technology on the employees?
	Q11	Do you know that there are any justifications for limiting employees' access to training?
	Q12	Are these limitations constructed legally?
	Q13	Is it legal to have limitations on the training in the company?
	Q14	If so, when and why should the limitation on training be enforced in the company?
Question related to	Q1	How was your company affected by the growth of technology such as cloud computing in the

regulation and policy;		industry?
	Q2	How responsive is the technology industry to have a changes in policy toward the employees' skill?
	Q3	Who, if anyone, do you believe to be responsible for the skills of the employee related to the growth of technology?
	Q4	Are you aware of any regulation or by law which deals with the growth of technology for employee?
	Q5	Do you believe that these laws and regulations work well in a practical context?
	Q6	Do you feel the current regulation and policy have protected the employee from the growth of technology?
Questions on how policy has supported the development of employees' skills	Q1	What responsibility do you have related to the policy on the growth of technology in the company?
	Q2	What is the basics step for the making of the policy in the company? Please provide as much detail as possible.
	Q3	What steps would you take to help this company achieve its objectives related to the growth of the technology in the industry?
	Q4	How do you prepare policies to deal with an underperforming employee?
	Q5	In your opinion, what practices are best to make sure that the allocation criteria used on the policy is objective to ensure equal treatment and to prevent discrimination and nepotism?
	Q6	At what point, if any, do you engage with the principle of transparency? When does it apply? Could you describe the use of the principle of transparency on making the policy in more detail?
	Q7	How are discrimination and nepotism being prevented? How is the equal/fair treatment of current employees ensured?
	Q8	To what extent is process of making a policy openly discussed at the managerial level?
	Q9	What steps would you take to ensure that a policy that you made will be successful?
	Q10	Have you used all available major resources that might improve your understanding or make your policy more effective?

	Q11	How do you know that the policies in the company are up-to-date?
	Q12	Are the skills of the authorized policy makers sufficiently to construct a policy in the event of growth of technology?
	Q13	Do you know how many policies have been change related to the growth of technology?
	Q14	What experiences have you had in policy-making related to the growth of technology?
	Q15	Are you aware of any relevant regulation related to the growth of technology?
	Q16	Do you think that current regulation or policy has accommodated and protected the need of employees in addressing any gaps in technology skills?
	Q17	Do you think that there is a need for reforming the current regulation or policy to cope with the growth of technology?
	Q18	Could you suggest any further regulation or policy that might protect employees in the light of the growth of technology?
	Q19	What do you think about corporate responsibility in company?
	Q20	Do you believe there is a role for using corporate responsibility to address any gaps in technology skills for employee?
	Q21	If company is using the corporate responsibility framework to accommodate gaps in high level technology skills, what, in your opinion, the approach would be?
	Q22	What benefits do you think for a company if using corporate responsibility framework to accommodate employees' gaps in high level technology skills?
	Q23	What problems do you think might rise if a company uses the corporate responsibility framework to accommodate employees' gaps in high level technology skills?

Closing We come to the end of the interview, I would like to say thank you very much for your time and attention. Do you have something to add or clarify about the interview or the research in general?

You can withdraw from the study, without offering any explanation, up to three weeks after the interview has been conducted. If you withdraw from the study, no data collected from withdrawing from the study will be used without your permission.

Would you like a transcript from this interview? If yes, I will deliver it to you in 2016 and I will send the summary of this research at the end of my research.