Cleansing Legacy Data for GDPR Compliance:
A Case Study

Harsha Pemmaiah Karthachira Chermana

A thesis submitted to the graduate faculty of Design and Creative Technologies
Auckland University of Technology
in partial fulfilment of the
requirements for the degree of
Master of Information Security and Digital Forensics

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand
2019

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

....

Harsha Pemmaiah Karthachira Chermana

Acknowledgements

I would like to express my sincere thanks to several individuals who have journeyed with me as I have worked on this thesis. I owe my supervisor, Professor Dr. Brian Cusack at Auckland University of Technology, my gratitude who has advised and supervised this thesis all throughout whenever I had some issues or had a question about my work. In addition, I must convey my sincere indebtedness to my wife Ashritha Kaveramma and to my parents for offering me constant encouragement and support during my study years and then through the analysis and development phases of this thesis. Without them, it would not have been achievable. I want to thank my mates, Subbaiah Thadiyangada, Poornima Raj and Namitha Shetty, for their invaluable recommendations. You offered me the tools I needed to choose the way forward and conclude my thesis confidently. Thank you.

Abstract

Today's news media are packed with information infringements and cybersecurity infringements amongst the world's most prominent companies. Misuse of personal information has become a major issue. Hence, the preservation of privacy and information is now more crucial than it has ever been. In May 2018, a major legislation was adopted in the European Union to tackle the problem of personal information privacy described as the General Data Protection Regulation or GDPR. Organisations these days collect immense amount of personal information in a quest to offer more personalised products and services. If collection is one part, the processing of information to offer better customer experience is the other part. However, the collection and processing of such personal information are not transparent as they go beyond the objective for which such data was obtained in the first place. On the other hand, malicious attacks are launched on organisations that collect a treasure trove of personal information. In either way, personal information is misused with considerable financial and mental distress to the victims. The GDPR was introduced to address all the privacy related issues to enable the right to privacy among the EU citizens. This legislation is also applicable to all other jurisdictions European citizens trade with.

Research Question: *How can the legacy data-sets collected by an organisation to comply with GDPR, be made compliant?*

Thus, the study goal of this thesis is to demonstrate the measures that organisations may adopt to comply with the GDPR. It is evident that all new information collected would have to follow the latest privacy mechanisms and the stringent compliance requirements of the GDPR. But the regulation is also applicable to the legacy data that organisations have in their possession. This becomes a herculean task to the organisations for regulation compliance. Any breach of data under the new regulation would bring sanctions and financial penalties on a large scale which could severely impact the regular operations of an organisation. Smaller organisations would probably disappear from the business environment. Through this study it is intended to demonstrate the management and technical controls adopted to address the cleansing of legacy data for GDPR compliance. A combination of management standards like ISO 27001, ISO 31000 and BS 10012, along with Privacy Enhancing Technology such as pseudonymisation will be used for the case study demonstration. I also understand the shortcomings and vulnerabilities in implementing the required mechanisms to comply with GDPR.

Table of Contents

Table of Figures

List of Tables

Chapter 1
INTRODUCTION

1.0 INTRODUCTION

Governments quite often establish or permit private firms to create public supervision mechanisms. Governments do so by using varying legislation on the pretext of national security to supervise or retrieve information from online mediums. Private businesses can collect various kinds of private data from active internet users to promote their product and services. They adopt various information acquisition techniques, such as data mining, crowdsourcing, internet surveying, etc. Such acts by private firms can pose significant threats to individual privacy. Various government authorities in developed nations have the necessary setup for using crowdsourcing to obtain private information. They obtain private information from people, who provided such information for a distinct purpose to a separate crowdsourcing service maintained by external parties (Diamantopoulou, Androutsopoulou, Gritzalis & Charalabidis, 2013).

In its entirety, the General Data Protection Regulation (GDPR) is referred to as the European parliament and council's regulation on the safeguarding of its citizens with respect to the processing of personal information and the freedom of movement of these information (Kammueller, 2018). The General Data Protection Regulation (GDPR), which has been in existence as of 2016 and as well as being compulsory from May 2018, lays out a new range of basic data protection principles, the rights of data subjects and legal responsibilities to protect EU citizens' personal information. This kind of legislative development influences the technical solutions to which they must adhere and the engineering procedure for the purpose which they have been created. For example, the solutions must introduce all the features necessary to help applications by the data subject to uphold their privileges. Such a legal strategy must be accompanied by technological provisions to safeguard data protection and private information. The ‘privacy-by-policy’ strategy makes the legal professionals responsible for adhering with the regulations. However, the specialists are not ready to cope with the associated requirements and the techniques to convert the requirements into software solutions. A practical strategy that offers advice to designers and technicians is required as an important contribution to efficient data privacy (Martin & Kung, 2018).

ISO 27001 can assist to satisfy the demands of GDPR through the following ways. 1) Assuredness: The GDPR proposes further use of accreditation systems like ISO 27001 as an assurance to ensure that the organisation manages its data security risks efficiently. 2) Not only private information: ISO 27001 employs global strategies that would assist businesses in setting up procedures that safeguard not just client data but all data resources, such as data held digitally and in printed format mode. 3) The structure and controls for security: The GDPR specifies that organisations must utilise suitable technological and operational controls to ameliorate the threats recognised, which ISO 27001 also recommends. 4) People, Processes and technology: Businesses may safeguard their organisation not only against computer-based threats, but also against more common challenges, including ill trained employees or inefficient processes. 5) Accountable: ISO 27001 requires that the security structure of businesses be endorsed by senior management and integrated into the lifestyle and policy of the company. It also involves the selection of a key person in charge of the information management system (ISMS). The GDPR clearly defines security and privacy liability throughout the enterprise. 6) Risk evaluation: Conformance with ISO 27001 implies periodic evaluations of risk to define challenges and weaknesses that may influence data resources of organisations and to establish measures to safeguard such information. Explicitly, a risk assessment is required in the GDPR to assure that an organisation has recognised weaknesses that may affect confidential information. 7) Continually improving: The ISMS implemented through ISO 27001 necessitates the businesses be continually tracked, revised and evaluated, thus evolving as the company progresses through a continuous improvement approach. It thus implies that ISMS should evolve as businesses continuously recognise and decrease threats. 8) Testing and inspections: Compliance with GDPR implies that an organisation must conduct periodic tests and inspections to demonstrate that its structure of security works efficiently. An ISMS that complies with ISO 27001 must be evaluated frequently which is consistent with the rules of internal audit laid down in the specification. 9) Certification: The GDPR needs companies to adopt the required measures to guarantee that the protective measures function as intended. Attaining ISO 27001 certification provides an independent, specialist evaluation as to whether the organisation has adopted appropriate data protection policies. (Lopes, Guarda & Oliveira, 2019).

ISO 27005 has been a well-known risk management system for information security. It is generally termed as Information Security Risk Management (ISRM). ISO 27005's functions typically involve identifying, assessing and prioritising the risks. ISRM must be a constantly reoccurring mechanism comprising of stages enabling continued improvement of decision-making and performance improvements when implemented correctly. Any organisation would be generating, collecting and processing substantial quantities of data in various forms throughout the risk management activities for information security. Information on risk management activities should be shared with all other interested parties to enable them to work together in risk management tasks. The organisation needs to recognise the information to be safeguarded and the level of protection to be applied. It is the duty of the organisation to protect and ensure the privacy, reliability and accessibility of sensitive data. Classification of information has been instrumental in organisational storage and exchanging of sensitive data (Agrawal, 2017).

The primary emphasis of information security is the implementation of technical protective measures to subdue malicious breaches. However, there seems to be a growing awareness of the fact that, despite such strategies, the future direction of an organisation eventually relies on its staff members' behavior. Internal staff members have reasonable and extensive access, apart from malicious outsiders, and can therefore cause chaos merely by making an error or performing an immature action thoughtlessly. Periodic exercises are performed to encourage maximum sensitivity of good practices among staff members. It is expected that such awareness-raising campaigns can help in the development of a culture of security so that good practice becomes the norm (Gundu, Flowerday & Renaud, 2019).

The significance of viewing privacy as part of the design mechanism of a system is commonly recognised as a significant element to the growth of privacy-conscious technologies. As an outcome, a variety of data protection measures have been implemented to help system engineers and architects in analysing and obtaining data protection demands for distinct software programs and distinct configurations. Because of the enhanced use of these techniques, it is becoming essential to assure that they do not only allow the creation and evaluation of privacy specifications, but also that that they are created with suitable functional elements to assure that they are implemented in the planned and relevant manner (Pattakou, Mavroeidi, Diamantopoulou, Kalloniatis & Gritzalis, 2018).

The basic criteria for privacy are taken as a key principle. The following were the criteria considered in the study. The first two criteria are primarily security considerations, but also because of their significant function in protecting privacy. 1) Authentication relates to the certainty that an individual's requested attribute is accurate.

Meeting this condition provides validation of the authenticity of an individual and guarantees the integrity of the data source. 2) Authorisation guarantees that approved personnel only shall handle the sensitive information of the individuals. It enables a verified individual to use a specific service, helps prevent breaches of the system integrity or resources of the account holder and prevents privacy breaches. 3) Anonymity is a property of data which does not allow the identification of an individually recognisable primary data explicitly or implicitly. Identity data will either be deleted or replaced all through anonymisation. 4) Pseudonymity is the use of an alias rather than an individually recognisable data. It helps individuals to access the service without revealing their identity. Utilising pseudonymity, a person might adopt several pseudonyms which helps in hiding their identity. Pseudonymity protects from the usage of internet facilities from unfortunate consequences. 5) Unlinkability is an individual's use of a service or system without the need for other stakeholders seeming to relate the individual to the service. It ensures the privacy of individuals while using a service or system by preventing illegitimate third parties from monitoring which services the individual uses. The assurance enables the threat of abuse of information relevant to privacy to be minimised and profiling prohibited or restricted. 6) Undetectability is a stakeholder's incapability to differentiate who is the individual customer of a service. It ensures the privacy of individuals while using a service or system by preventing unauthorised third parties from detecting which resources the customer is using. 7) Unobservability is a third party's incapability to control the use of a service by an individual. It guarantees that an individual can use a service or system without being able to notice that the service or system is being used without someone, particularly third parties. It also needs individuals and/or participants to be unable to determine if an activity is being carried out (Diamantopoulou et al., 2013).

A critical desensitisation method is pseudonymisation, where unique identification of facts, for example tax ID number, credit-card numbers or combinations of traits, e.g. phone numbers and addresses, is substituted by a randomly-looking alternate, the pseudonym. Pseudonymisation is a commonly used method for de-sensitising information pieces by replacing the identifiable characteristics with non-sensitive alternates continuously. In order to sustain the usefulness of the information, all occurrences with the same unique identifier must always be substituted continuously with the same pseudonym. NIST recommends pseudonymisation for private data privacy and has even been authorised in a variety of industry-specific laws. Such powerful laws extend to private information, and the GDPR officially advocates pseudonymisation as a lawful means of removing information identity. The GDPR, for example, allows the processing of pseudonymised data for functions beyond the intent for which the data were primarily gathered (Lehmann, 2019).

The information collection architecture helps determine which information items are gathered and whether an auxiliary or required information item is gathered. The structure of the information also covers the objective and period of retention for every data element. Quite often the data gathered is circulated with other organisations. An organisation does not have to implement a standardised structure of privacy to all its users. Personalised privacy designs can be useful to users, as understanding and trying to prevent online users' privacy choices can ease the strain of customising privacy controls individually. The advancement of personalised privacy concepts also opens the possibility of user-company agreement (Preibusch, Kübler & Beresford, 2013).

Through the research case study, it is intended to demonstrate the cleansing of legacy data for GDPR compliance. A brief review on the requirements of GDPR will be performed to understand the intricacies of the legislation. The case study implementation ideology combines the information from ISO 27001 (Information Security Management System), ISO 31000 (Risk Management) and BS 10012 (Personal Information Management System) standards. These standards provide the best practices and guidelines to form a framework of activities to be performed within an organisation in order to achieve the privacy and security objectives. As privacy is achieved through a robust security, the ISO 27001 standard enables to create a blueprint of the measures that must be adopted in the organisation to implement security mechanisms. The ISO 31000 enables understanding of the risk management framework. It enables the Privacy Impact Assessment (PIA) which in-turn means that an assessment of the risks needs to be performed because of the risks posed against privacy. The BS 10012 standard enables a fusion of both former standards to achieve compliance towards GDPR. The GDPR has provisions for certification mechanisms to enable organisations to portray their GDPR compliance, and BS 10012 is one of the standards created to cater that purpose. Based on the principles and guidelines laid down by the GDPR, the case study will be focusing on achieving privacy and security through implementing Privacy by Design (PbD) by adopting Privacy Enhancing Technology (PET). For demonstration purposes, two publicly available data sets are used. The technology that is planned to be adopted is pseudonymisation which enables the masking of the data. To be compliant with GDPR, it is not enough that technological measures alone would enable compliance. There are behavioral factors of individuals too which contribute to the adherence of requirements. Cleansing of legacy data is a time consuming and continuous process as the regulation requires organisations to keep a track of all the personal information collected and service the rights of the EU data subjects.

Chapter 2
LITERATURE REVIEW

2.0 INTRODUCTION

Data protection is more essential now than ever before and people are far warier of the privacy of their financial and personal information and are more attentive. The widening number of high-profile businesses in the headlines, such as Target and Home Depot, and the recent misuse of customer data by Facebook continue to increase data security problems (Wright, 2018). Modern systems store data that affect global citizens' lives. So far, little or no supervision has been exercised over how such information is stored, managed, archived or eventually destroyed. Our personal information is sometimes sold from company to company without our knowledge. It could be used to deliver us with smarter products and services, but it can also sometimes jeopardise privacy rights or be used for malicious purposes (King-Bailey, 2018).

Within the regulatory outline of the privacy act, the GDPR is the *lex generalis* (law applicable to all). It has brought benefits for businesses and citizens alike. On the one hand, individuals have now been given new tools to enable them to exert command upon the data that they generate. From another point of view, data controllers have all been required to comply with the data protection concept by design and as a standard. The recently formed European Data Protection Board has been empowered to issue legally enforceable decisions in the event of disputes between national data protection bodies, as well as the issuance of GDPR implementation directives. The GDPR lays down strict guidelines on the circumstances for administrative penalties for business entities that do not meet the current EU rules (Kędzior, 2019).

Privacy by Design (PbD) arises from work that is done by the office of the Ontario Information and Privacy Commissioner in the mid-1990s. The principle of Privacy by Design (PbD) was further demonstrated by the GDPR in Article 23, in which it was pointed to as data protection by design. Pseudonymisation and data minimisation are a welcome step, that suggest a standard for designing and implementing PbD. Not only does the law require the online mechanisms to be privacy compliant, but they must be carefully reproducible. Privacy by Design is a framework in which legal / constitutional scholars and system developers need to continually work together (Diver & Schafer, 2017).

The GDPR has a wide geopolitical reach, which means it influences non-EU companies. For non-EU businesses, privacy and information protection did not matter up until the enforcement of GDPR. These new regulations will affect any multi-national organisation that handles the private information of every individual who resides in the European Union. Every handling of private information within the scope of an EU branch or subsidiary must be in accordance with the GDPR. In addition, all businesses with European Union clients or businesses that only monitor the behaviors of individuals living in the EU, must comply with the regulation regardless of physical location. The critical factor is not where the data processor or data controller is located, but where the individual (data subject) is located (Mueller, 2017).

GDPR affects people, processes and technology at a very high level. Technology must provide the capacity to protect and defend personal information by implementing appropriate management of archiving, retaining data, erasure capabilities, along with identity and access management. Processes need to assure data is controlled across its life span. Finally, people need to be trained and made accountable for data management. Its fundamental assumption is that the computer systems of today must be designed to provide privacy, commonly referred as 'privacy by design'. Performance in the digital realm of today relies on how well personal information is managed and validated. Every day, validation professionals strive to validate systems worldwide in accordance with current regulations. Quite enough emphasis is on the gratification of systems from a test perspective to help make sure that systems follow their designed usage. People throughout the world must always be watchful about knowing how data is managed and asking for the right to be forgotten if needed (King-Bailey, 2018).

The key role of personal information and the worldwide aspect of processing requires appropriate safeguards (Wolters, 2017). The right to portability of data in the GDPR would necessitate companies to ensure they are able to deliver personal information in a transferable and functional manner supplied by a person. If businesses are controllers of data and handle private information, portability of data would cover a broad range of fields including social networking sites, web-based search, online storage, online stores, online banking, emails, health insurance companies, power companies, aviation companies, and smaller businesses including pizzerias and dressmakers (Vanberg, 2018).

Conformance to GDPR will require ongoing time and attention. Internal audit can enable the organisation to reduce the risks of compliance with GDPR by assessing ways to improve controls, raise awareness of risks and ensure compliance. Specifically, the regulation necessitates organisations to concentrate on control-oriented issues such as accuracy and quality of data, security and privacy through design and security. GDPR's direct risks relate to probable penalties and reputational affect (Hertzberg, 2018).

2.1 PRIVACY AND ITS RELATED RISKS

There are dissimilar and contradictory views on privacy. Some argue that privacy must be treated as a basic right and few others contend that privacy is not a fundamental tenet compared to life's values. Some others believe that sharing of information and privacy are dependent on context, which means that the aspects like category of information, beneficiary and purpose of information amid others impact the willingness of an individual to disclose (Bhatia & Breaux, 2018). Human dignity and autonomy are firmly entrenched in the understanding of privacy by the EU. It means that everyone can control and draw the line between their formal and informal domains (Mueller, 2017). Data privacy emanated as a basic right in the European Union when Germany adopted the first information privacy act in the world. Later privacy of information was established in each Member nation and then at EU level, and it became the most stringent and significant information privacy administration in the world. Data privacy has become transnational. Such a new globalised ecosystem gives little confidence to domestic territorial data protection laws (Azzi, 2018).

Management of risk is used to recognise, assess and prioritise the risks and develop effective techniques to minimise risk. Individual users are concerned about privacy risk because of their behavior and association with other aspects, while risks related to security are threats postured by opponents attacking or threatening a structure. Under risk management for privacy, methods and approaches including categorisation, prioritisation of risk and the establishment of risk reduction collaboration methods are used by designers to manage privacy risks. Designers may not always predict the notion of an individual's risk of privacy, nor must the designers inherently consider all private information as too risky. The privacy impact assessment is a tool to make decisions that allows businesses and administration establishments identify and decrease risks related to privacy through data management (Bhatia & Breaux, 2018).

For many entities, data has become an asset, offering better business activities and new business prospects. Also, collection of data has multiplied the access to sensitive information that can threaten the personal information of people and breach of laws related to protection of data when processed. For that reason, controllers of data and processors of data could be subjected to severe sanctions for non-compliance, which can lead to going bankrupt (Gruschka, Mavroeidis, Vishi & Jensen, 2018). Privacy risks could be the result of poor data collection mechanisms, storing data inappropriately, and information disclosure. The associated security threats could be such as no encryption of data, device vulnerability and breach in data security. A combination of privacy risks and security threats can result in severe penalties (Sampat & Prabhakar, 2017).

In 2015, the Global Privacy Enforcement Network, consisting of data protection authorities from all over the world, conducted a sweep of applications and sites targeting or prominent with children. Sweepers concluded that children who use 41 percent of the sites reviewed would be vulnerable. They have included their concerns such as excessive collection of personal information, lack of language that kids might understand, disclosure of data on ambiguous or undisclosed grounds to external parties and unmonitored chatrooms used by children to share excessive personal information (Atkinson, 2018).

With both privacy law intrusiveness and non-compliance penalties increasing, entrepreneurs are becoming increasingly worried with how best to manage conformance, not only in terms of cost but also efficiency (Mitchell & Fondi, 2018). While transferring information from a controller of information to another, security and privacy doubts emerge. Interestingly, according to the GDPR, interoperable approaches might exacerbate security issues at the cost of procedures and uniform instructions. This is a major concern, especially for small to medium enterprises (SMEs) having resource constraints to spend on security and privacy. There might be circumstances at which a controller of information must be entitled to deny portability of information due to security apprehensions at the reception side (Vanberg, 2018).

Research has shown that cyber privacy risks have a negative impact on several individuals who share private data for services from online providers and internet transactions (Wang, 2019). Nowadays, businesses have found new approaches to commercialising customer data and privacy to manipulate increasing data sharing demands and subsequent privacy risks. One such approach is the pay-for-privacy (PFP) model, that enables companies to charge higher premiums to minimise collecting data and targeted advertising, whereas cutting prices to customers who give permission to such practices. At the same time, the Personal Data Economy (PDE) has become a user-centered data principle that allows individuals to own their data, so they can then divulge it with companies on their own contractual terms. Models like PFP and PDE generate critical apprehensions regarding collection of data, privacy and consumer involvement in the data business (Elvy, 2017).

2.2 THE REGULATION

The regulation comprises of 99 articles which are clustered into 11 chapters, as described in Table 2.2.1 (General Data Protection Regulation, 2016).

Table 2.2.1: Chapters highlighting the regulation (GDPR, 2016)

Chapter number	Chapter name	Articles covered
1	General provisions	1 to 4
2	Principles	5 to 11
3	Rights of the data subject	12 to 23
4	Controller and processor	24 to 43
5	Transfers of personal data to third countries or international organisations	44 to 50
6	Independent supervisory authority	51 to 59
7	Cooperation and consistency	60 to 76
8	Remedies, liability and penalties	77 to 84
9	Provisions relating to specific processing situations	85 to 91
10	Delegated acts and implementing acts	92 & 93
11	Final provisions	94 to 99

2.2.1 General provisions

The GDPR's purpose is to safeguard the personal information of EU nationals. The Commission enacted the regulation in such a way that emphasises the actions of the operator, which follows a destination-based strategy applicable wherever data from EU is being processed. The applicability of EU rules to operators outside the EU who processes the EU personal information are in two situations. First, when dealing the supply of outputs offered by businesses in the EU. Secondly, where the monitoring of people's behavior in the EU is concerned (Azzi, 2018).

The GDPR states that if an organisation holds personal information, those entities should therefore acquire adequate authorisations. Businesses receiving second-hand information must demonstrate the need for it (Elkins, 2019). Among the six lawful bases for the processing of data, consent one of them. A person consents to the use of his or her data for as much relevant considerations. Rights of the individuals are also stated as the controlling rights. The information rights are a significant controlling factor, readying the individuals for and its implications for data processing. Consent is valid only if the data processing is approved or disapproved by the individual (van Ooijen & Vrabec, 2019).

The GDPR directly imposes the personal data protection obligations on the controller of data and the processor of data all over the EU. The data subject partially enforces these obligations. The GDPR generates and reinforces numerous rights that give the EU citizens the command regarding private information processing. The GDPR also gives the citizens several enforcement rights. These rights enable EU citizens to enforce the regulation through a supervisory authority or court of law (Wolters, 2019).

2.2.2 Principles

There are six principles; namely (General Data Protection Regulation, 2016)

i. Lawfulness, righteousness and openness – processing of the personal information in relation to the EU citizens shall be performed legally, fairly and transparently;

ii. Purpose limitation - collected for specific tasks so as not to process in an inconsistent manner with any of those aims;

iii. Information minimisation - the purpose with which they are processed is necessary, important and limited;

iv. Accuracy – precise and current, and facilitate the prompt removal or rectification of incorrect private information;

v. Limiting storage - kept in a format that allows the identification of data subjects for the intent for which personal information are processed no longer than is necessary;

vi. Integrity and confidentiality - processed to ascertain enough security of private information, particularly safeguarding from unlawful or unauthorised processing and unintentional destruction, degradation or harm, by effective technological or organisational initiatives

Not only does the GDPR require a lawful basis for activities like processing, but it also exists to serve as a legitimate ground for several different processing activities. Controllers who are unable to find a correct legal basis for their tasks beyond the scope of the GDPR may look up to the GDPR and attempt to focus exclusively under one of the six principles mentioned in Article 6. Before processing begins, the controller must ascertain the legal basis and document it. The selection of the most appropriate legal basis must be a component of an organisation's data management strategy and therefore should be thoroughly evaluated by all interested parties in the decision-making process. Consent must be given freely, specifically, informedly and indisputably. The necessity for explicit consent is linked to fairness, transparency and information requirements of data protection principles. Consent also need to be extremely clear and a positive action must be taken to exclude pre-ticked boxes from GDPR specific rules. Exceptional categories of data require written consent, rather than any other positive action. (Gil González & de Hert, 2019).

GDPR requires requests for consent to be 'opt in' rather than 'opt out'. Also, withdrawing consent must be as convenient as giving it (Astrup, 2018). According to the GDPR, if consensus is used as the rationale for the personal information processing, only children above a certain age (to be determined at country level) can give their own consent. It will be necessary to seek and verify consent from a bearer of parental rights who are below the age of digital consent (Atkinson, 2018).

2.3 RIGHTS OF THE DATA SUBJECT

The GDPR establishes multiple liabilities for processors and controllers of personal data. Only if the processors and controllers fulfil their obligations will this lead to the safeguarding of private information. GDPR implementation relies primarily on the supervisory authorities of each Member State (Wolters, 2018). It will be essential that the controller assures the outside world clearly and transparently about the processing in a lawful manner. In any event, the citizens have the authority to revoke their consent for processing (Gil González & de Hert, 2019).

2.3.1 Right of access by the data subject

The citizens are entitled to receive notification from the controller on whether the personal information is being processed or not. The regulation entitles the citizens to a replica of the processed data. Furthermore, the controller shall offer good information on any of the data and the processing activities. Such information must be provided in a straightforward, clear, readable and readily available manner using a simple language. The controller must inform the citizens of the retention period contemplated or the definition of what constitutes the retention period. The controller must notify the citizens of their other authorities and the option of filing a lawsuit with the supervisory authority (Wolters, 2018).

2.3.2 Right to rectification

The citizens do have the authority to rectify erroneous private data relating them from the controller. They are also entitled to finalise the information if they are inaccurate in view of the processing purposes. The regulation requires the controller to inform the beneficiaries to whom the personal information was made available of the rectification or completion of information. The citizens are subsequently eligible to details about the beneficiaries. The principle of accuracy exerts an overall obligation to make sure fullness and reliability of the information (Wolters, 2018).

2.3.3 Right to erasure (‘right to be forgotten’)

The citizens are entitled to extract the erasure of personal information addressing them from the controller. If the data is disclosed at large by the controller, the regulation requires the controller to initiate suitable actions to notify other controllers of the query to erase private information. The GDPR enforces an obligation to report the erasure of the beneficiaries by the controller to whom the personal information was made available. The controller would be responsible for both the observance of the principles of minimisation of data and limitation of storage (Wolters, 2018).

2.3.4 Right to restriction of processing

The citizens would have the authority to attain restrictions on the processing of their private information from the controller. The controller hereby processes the data with the consensus of the data subject for the purposes of establishing, upholding or responding civil lawsuits, protecting the rights of another person or for factors of best interest of the public. The controller is still permitted to keep the personal information. The GDPR creates an obligation by enforcing the information controller to divulge the restriction to the beneficiaries with whom the personal information was made available. The right may be a short-term fix if the validity of personal information is in dispute. The authority to limit the private data processing may be an option if the data subject requires them in connection with a legal complaint or objects to the erasure of wrongfully processed data for a different purpose (Wolters, 2018).

2.3.5 Right to data portability

The citizens can collect a copy of private information. The GDPR asserts that the citizens are eligible to pass the information on to some other controller. The authority of porting the information reinforces the citizens' control of their information. It also lets the citizens to port their information to certain other new controllers rather than simply trying to influence the processing by current controllers. The right extends only to personal information supplied to the controller by the citizens and would not include information generated by the controller. The data portability right is accomplished only when computerised processing is carried out (Wolters, 2018). Data portability complements the right of access of the citizens. The authority on porting of information provides the citizens a simple way to handle and repurpose personal information (Chirica, 2017).

2.3.6 Right to object

The citizens will have the authority to oppose their private information being processed. The regulation gives the citizens the authority to oppose to information being processed for applications marketed directly at any time. If the citizens exercise this right, the information for these applications will therefore not be processed. This right need to be exercised based on reasons related to the citizen's specific circumstance. The controller is obliged to discontinue data processing only if the objection is validated. The regulation would not establish the authority to oppose to the scientific processing or empirical research or statistical activities (Wolters, 2018).

2.3.7 Automated individual decision making, including profiling

The GDPR specifies that a citizen is entitled to not be subjected to decisions purely based on computerised analysis or categorisation that will have implications legally on them or would be affecting them equally substantially. In fact, this right is a restriction. The restriction would not be applied if the action is essential to draw the conclusion between the citizen and with the data controller or to carry out the agreement (Wolters, 2018).

2.4 CONTROLLER AND PROCESSOR

The controller is an inherent or statutory individual, government body, authority or any other agency that defines the objectives and methods for private information processing by themselves or in conjunction with others. The processor is a natural or statutory individual, government body, authority or a supplementary entity that processes private information on behalf of the controller. According to GDPR, whoever intends to process other individual's personal information becomes a controller. If the data is used for business purposes without following the guidelines of the controller, the processor would become a controller. Thus, the controller and perhaps even the processor are the participants responsible for the safeguarding of private data (Ungureanu, 2018).

GDPR incorporates two new approaches concerning to the private information processing: the first is the idea of 'privacy by design' and then second is 'privacy by default'. Relevant operational and technological initiatives will therefore be employed by the controller during the decision-making moment and while processing, this is referred to as privacy by design. The controller ensures that only the private data required for each processing objective is explicitly processed with respect to the quantity of the information gathered, the level of processing, duration of retention and availability of the data gathered, this is referred to as privacy by default (Chirica, 2017).

Data Protection Officers (DPOs) are the backbone of compliance for protecting information in the GDPR's context. A DPO is an individual, maybe an employee or a contractor, who would be formally accountable for compliance with protecting information within a government body or an enterprise. The controller must appoint a DPO, but it is not necessary for the processor to appoint another. Where a government body or business carries out the specific data processing operation, a DPO shall be appointed. The DPO function may be performed either by an independent staff or by an organisation external of the processor / controller. To carry out its tasks effectively, the DPO must have ample freedom and adequate resources (Cliza & Spataru-Negura, 2018).

GDPR has introduced the idea of data protection impact assessment. The impact assessment would be implemented when the processing is inclined to pose a significant risk to natural persons' liberties. The criteria for processing the need for data protection impact assessment are such as aspects of profiling, automated decision making, systematic monitoring, sensitive data, data transference across the border, and so on. The more criteria a processing activity meets, the more apparent it becomes that the impact assessment of data protection is needed. This impact assessment is executed before the processing starts. The data controller is liable for the impact assessment on data protection (Chirica, 2017).

2.5 TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

According to GDPR, the word cross-border processing comprises the processing of private data concerning the operations of businesses in one or more Member States of both the processor or controller in the Union wherein the processor or controller is situated in one or more Member States. It also involves the private information processing in connection with the operations of a sole organisation of a processor or controller in the Union, and that would impact or would possibly impact citizens significantly in one or more Member States (Ungureanu, 2018).

Corporate tech giants have been so formidable that they are proficient in accumulating, transferring and analysing private information from account holders' internet activities around the globe. The transfer of the EU information to foreign nations implies that a controller of data within the EU gathers information and then sends that information to the foreign country processor or controller. There are some difficulties in the legal details of data transfer to foreign countries. A fundamental principle is that until the actual exchange occurs, the regulations of the nation from which the information is gathered applies to the controller (Bu-Pasha, 2017).

With a comprehensive international activity, non-compliance by a single entity would have a major effect on the entire collective turnover of MNCs. Considering the intense financial implications of the new regulation, it is recommended that Binding Corporate Rules (BCR) be adopted to enable data transfer within the group entities. An evaluation of the risk assessment mechanisms is essential to analyse the genuine transfer of data. If data were not transferred on a reasonable basis, the financial health of the company could be severely damaged, resulting in adverse publicity (Ungureanu, 2018). A movement of private information to a multi-national organisation or a foreign nation might be carried out where the Commission has determined to ensure that an adequate measure of security for a foreign nation, a region or at least one specific sector is available within that foreign nation or multi-national organisation. No specific authorisation shall be required for such a transfer. To date, the European Commission has acknowledged Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United

States of America (restricted to the framework of the Privacy Shield) as offering acceptable safeguards (Official Journal of the European Union, 2016).

2.6 INDEPENDENT SUPERVISORY AUTHORITY

Supervisory authority is an autonomous government agency set up by a Member Nation. The supervisory authority would be accountable for data protection measures in most of the situations (Calder, 2018). Every supervisory authority shall carry out its duties and exercise its abilities with greater autonomy, which includes investigative powers, corrective powers, authorisations and consultative powers. Member Nations should ensure the appointment of their supervisory authorities through a transparent procedure. The Supervisory Authority must publish a summary of processing operations including an impact assessment of data protection. The Supervisory authority must receive the communication particulars of all the Data Protection Officers (DPOs) from the controllers or the processors. The DPO would be the intermediary contact point between the organisation and the Supervisory Authority (General Data Protection Regulation, 2016). The transfer of information to countries that are regarded to have unsatisfactory security levels is forbidden, except if authorised by a supervisory authority. It necessitates that the data transfer contracts be negotiated (Tankard, 2016).

To determine the adherence with this legislation, the supervisory authorities must promote the creation of an information protection certification mechanism. Each supervisory authority must assist in submitting of complaints through provisions such as a form for submitting the complaints that can also be accomplished through online mediums, with no barring of any other contacting mediums. For the citizens and, where appropriate, for the data protection officer, the performance of each supervisory authority's tasks must be free of cost. All data breaches shall be reported to the Supervisory Authority within 72 hours of being conscious of the of the incident. If there is a delay, then suitable reasons must be provided. Each supervisory authority's members and staffs are bound to legal confidentiality both during and after their duration of service, in respect of any sensitive data that has come to their notice while performing their tasks or exercising their powers. Every supervisory authority shall prepare a yearly report around its tasks, that may include a list of breaches and forms of action on them. Every supervisory authority shall adopt all necessary steps to respond to another supervisory authority's request without delaying the response (General Data Protection Regulation, 2016).

2.7 REMEDIES, LIABILITIES AND PENALTIES

Privacy and personal information protection are not just protecting personal interests, they also safeguard the benefits of the population. That is why it is the Government's job to safeguard private information. A citizen shall have the authority to file a grievance with the supervisory authority if he finds that the processing of his private information violates the regulation. A supervisory authority must make grievance submission easier by providing an electronic complaint form. The complaint will be handled free of cost. The supervisory authority might collect fees or take no action only if the application is clearly unjustified or overwhelming, in short due to its repetitive nature. A data subject may file a complaint at his habitual residence, workplace or place of alleged breach with the supervisory authority (Wolters, 2019).

A data subject is entitled to efficient legal redress against a supervisory authority. The data subject has this right if the complaint is not handled by the authority or the data subject is not made known of the development or result in three months. If the grievance is rejected by the authority, data subjects may bring proceedings in contradiction of a legitimately enforceable judgement of the supervisory authority affecting them. The GDPR contains no rules on the fees and duration of the legal proceedings. Some Member States restrict access to an appropriate legal solution. It reinforces the data subject's position by clarifying the type of decisions to be appealed and the jurisdiction of the courts (Wolters, 2019).

The processing of personal data happens on a broad scale. It is virtually impossible to monitor all processing operations even if the supervisory authorities' budget is expanded. The GDPR therefore grants the citizens the authority to an appropriate legal redress opposing a controller or processor if it is perceived that rights have been violated. In most cases, the data subject can pursue charges before the tribunal of his habitual residence because of him being a victim as an end user or a staff member (Wolters, 2019).

Many data subjects can impose the rights through an organisation. This minimises legal expenses per data subject and enhances his direct exposure to expert legal representation and other expertise. The GDPR grants the data subject the ability to pursue the rights through a non-profit entity. The GDPR states that such entities also have its own right, nonetheless of the mandate of the citizen. It empowers an entity to lodge a grievance with the Member State's supervisory authority in which it is established (Wolters, 2019).

A citizen who has sustained physical or technical issues because of a GDPR violation shall be entitled to emolument from the processor or controller. The data controller is ultimately in charge of the processing and is accountable for the entire damage. When more than one controller or processor is accountable for that very same violation, any of the data subjects may claim full compensation. A processor or controller must be immune from accountability once it demonstrates that they are not responsible in any way for the damage caused (Wolters, 2019).

A 2014 research by the European Union Agency for Fundamental Rights found that many of the most recurrent reasons of personal information breaches were due the data subject's Internet activities, such as social networks, online contracts like online shopping, email accounts, abuse of personal information by global Internet giants. The next reason was deemed to be the profiling and selling of personal information to external parties by controllers or processors with no consensus from the citizens. Typically, the damages suffered by data subjects concern a large group of people (Ungureanu, 2018).

The GDPR commands that any infringement of information must be reported under 72 hours to the Supervisory Authority and businesses must also notify the persons concerned if the infringement has a substantial impact on them (Astrup, 2018). What worries several entities is the likelihood of everlasting financial sanctions if they breach the GDPR. A non-compliant business could be penalised up to €20 million or 4% of its global income, depending on which would be high. A breach need not occur to invoke the penalty. Member States may impose penalties more than the GDPR penalty. An entity that does not comply is also susceptible to civil lawsuits. A lot of companies and industries which have never cared about data protection earlier would be at a mammoth financial risk (Elkins, 2019).

2.8 COMPLYING WITH THE REGULATION

Apprehensions related to the security and privacy of data are increasingly making compliance with the General Data Protection Regulation (GDPR) more crucial than it was before. First, it is necessary to conduct an internal gap assessment or recruit competent professionals to review the existing system, policies and processes and recognise issues that need to be resolved quickly. Second, evaluate what personal information the organisation holds about European Union (EU) citizens. Identify exactly where these data are stored, where they are hosted, when they were last used, and what they were used for. Take a glance at the processes that are in place for data protection.

Third, evaluate if personal information was exchanged with certain vendors and associates. If so, make sure that such entities can use those data and do their best to adhere within the GDPR provisions, and review contracts appropriately. Fourth, begin with queries and requisites for compliance with GDPR in RFPs. Finally, describe simple methods that may jeopardise information security. Consider all those encountering every kind of private data are conscious of the significance of irresponsible personal data handling (Ross, 2019).

Privacy by design requires incorporating privacy protection into technology, business models and physical infrastructure technical requirements. A mechanism which enforces privacy by design fundamentally complies with data protection laws. This adoption requires the acknowledgement of all the design stakeholders. It is not just a matter of IT security anymore; the entire design framework will have to keep privacy at the forefront. The Privacy Impact Assessment would also help in determining the impact of privacy risks. The product of an impact assessment of privacy is the mitigation and management of risks related to privacy by anonymising, pseudonymising or aggregating the databases. The cost of a weak privacy design is large (Featherstone & Miller, 2018).

Disclosure of infringement and Subject Access Request (SAR) vigorously demonstrate a requirement to train all staff so that they will be attentive of the problems and would know how to recognise what an infringement and SAR is. In less than 72 hours of it being noticed, breaches must be notified. SARs means the requisition for a copy of personal information of a certain person may be sent to someone in the company, without the necessity for them to go to the risk / privacy department or, for example, to the HR. All employees need to know how and when to locate a SAR and where to direct it. SARs appear to tend to circumvent statutory authority, and hence it is better to involve the legal experts in the learning program. Training must also ensure that, when a new managerial process or a technical process that impact personal information, an up to date record of the processes performed needs to be maintained. They must also be aware that a Privacy Impact Assessment (PIA) is required in some cases. Training is an ongoing process and there is a need to cover existing employees and new people joining (Doe, 2018).

Personal Information Management (PIM) is becoming a growing subject in the field of information recovery, where it contributes significantly in the supervision and recovery of personal data. It includes techniques and processes for storing, managing, collecting and displaying information such as documents, emails, web pages and digital media information. Tools are needed to lower the difficulty of information management challenges faced (Nasar & Mohd. & Ali, 2011). Privacy is consistently attained through anonymisation and cryptography to deter deceptive people from accessing information. A security framework cannot always assure privacy as it focuses more on deterring malicious access. Information Management Systems demonstrate fruitful outcomes in terms of privacy, as they evaluate the contextual effects of all actions taken (Jayasinghe & Lee & MacDermott, 2018).

In several organisations, GDPR prerequisites are described as methods or practices which are to be incorporated into the commercial operations. The organisational context provides a reason to seek an option to apply the ISO 9000 family of standards as a process for implementing the GDPR. The process perspective adopted in the 2015 standard update necessitates organisations to manage their processes to attain the intended outcomes aligned with the organisation's strategic objectives. ISO 9001:2015 now needs organisations to recognise, register, adopt, sustain and enhance processes and correlations continuously. GDPR encourages the application of standards as evidence of adherence (information security ISO 27001, cloud processing ISO 27018) and as a process for achieving various requisites (risk management ISO 31000). The accreditation or voluntary regulation philosophy is often centered on the application of generally recognised standards. At the framework stage, the standards can be used as a methodology (ISO 9001: 2015), for a process to complete the various phases (ISO 31000), or as a certification of conformity with the legislation (ISO 27000 (27001, 27017, 27018)) (Tzolov, 2018).

The British Standards Institution has formulated the BS 10012:2017 standard based on the ISO management system structure to conform with the European Union General Data Protection Regulation (GDPR). The standard formulated adopts the familiar PDCA (Plan, Do, Check, Act) model. The ‘Plan’ phase involves the context of the organisation, leadership, planning and support related requirements. The ‘Do’ phase involves the operation related requirements. The ‘Check’ phase involves the performance evaluation related requirements. Finally, the ‘Act’ phase involves the improvement related requirements. The standard consistently relies on the ISO/IEC 27002:2013 for the implementation of managerial and technical controls necessary for a robust Personal Information Management System (PIMS) in an organisation. To address the risks, it advises to rely on the ISO 31000 standard. Almost all the personal information could fall throughout the scope of other organisational management systems such as ISO 9001, ISO 14001, ISO 55001, ISO/IEC 27001. Consideration should be given to use a common management system framework if organisations have various overlapping management systems (BSI Standards Limited, 2017).

Following are the details of the high-level requirements that the BS 10012:2017 standard recommends: (BSI Standards Limited, 2017)

Context of the organisation: It intends to enlist the external and internal issues to an organisation in relation to the private data. It expects it identify the intended parties related to the personal information management system. It requires the scope for PIMS to be defined precisely. Based on these agenda, the Personal Information Management System for an organisation is developed

Leadership: It requires the top management to demonstrate its commitment and leadership initiatives towards the PIMS. It requires the leadership to formulate a PIMS policy. The leadership must ensure that the roles, responsibilities and authorities are described and communicated. The leadership must ensure that the culture of PIMS is embedded firmly within the organisation.

Planning: The organisations must plan to address the risks and opportunities. They shall plan the processes required for managing the data inventories and the flow of data. They shall confirm that the processing is done according to the statutory or regulatory requirements; especial where special categories of personal information is involved. They must establish a process to perform privacy impact assessment. They must establish the process for privacy risk treatment. If certain privacy risks are not mitigated, then they must be consulted and authorised by the supervisory authority. All the systems used for internal purpose or to provide products / services externally must follow privacy by design and by default. The organisations must formulate the objectives related privacy and the mechanism to achieve those objectives.

Support: The organisations shall allocate the required facilities for creating, realising, sustaining and continuously enhancing the PIMS. Adequate awareness and training shall be imparted to all the employees. Relevant information must be conveyed to internal and external parties regarding the PIMS implemented. Hard data in terms of documents must be sustained where necessary. The documents created and updated related to the PIMS must be controlled in an adequate manner.

Operation: As per the requirement of PIMS, the organisations must plan, implement and control the processes required. A top management representative must be appointed as accountable for PIMS. A DPO shall be appointed. Each department within an organisation shall identify suitable data protection representatives. Privacy risk assessment and treatment must be performed. Awareness trainings must be imparted. Data process must be performed fairly, lawfully and transparently. Records for consent and the purpose for processing must be maintained. All the principles of GDPR must be carefully adhered through adequate processes. Security issues must be resolved through adopting necessary controls.

Performance evaluation: Organisations must supervise, quantify, review and assess the implementation of PIMS with respect to the objectives defined. Internal audits must be performed at pre-defined intervals. The top management must review the PIMS implementation to make sure that it is adequate and effective.

Improvement: Organisations must address non-conformity of any sort with utmost priority. Where applicable, necessary corrective actions must be implemented. Potential non-conformity must be addressed through adequate preventive measure. Organisations must consider the outcomes of performance evaluation, non-conformities, corrective and preventive actions to continuously improve the PIMS.

2.9 A BRIEF COMPARISON WITH THE NEW ZEALAND’S PRIVACY ACT

New Zealand decided to move quickly to enforce the Organisation of Economic Cooperation and Development’s (OECD) initial principles of privacy into the New Zealand Privacy Act 1993. From the beginning, the Privacy Act was applicable to the corporate sector only. Since May 2018, the Privacy Act is applicable to institutions or persons from public or private sector who may or may not have been incorporated (Ingley & Wells, 2018).

There are 12 Information Privacy Principles (IPPs) according to the New Zealand Privacy Act 1993, which are as follows: (Privacy Act, 1993)

- Objective of private data compilation – the legalised collection of information for a definitive purpose
- Origin of private data – the data shall be gathered straight away from the concerned person
- Collection of data from subject – the concerned individual shall be notified on the collection, reason for collection and possible recipients of personal information
- Ways of private data compilation – the data collection shall not be unlawful, biased or unreasonable
- Security and storage of private data – the data collected shall be secured by the entity engaged in the information collection activity

- Access to personal information – the entity shall enable easy retrieval of the personal information that it is holding
- Correction of personal information – the entity shall enable rectification of the private data that it is holding
- Integrity of private data to be examined prior to using it – the entity shall ensure that the data held is correct, reliable, complete, appropriate and not deceptive
- The agency should not retain private data longer than needed – the entity shall not hold the private information for activities beyond the required purpose
- Limits on usage of private data – the organisation holding the private data shall not repurpose the existing information without legitimate reasons
- Limits on revelation of private data – the organisation holding the private data must not reveal the existing data beyond legitimate reasons
- Unique identifiers – the entity shall not assign any sort of distinct credentials to a person

The New Zealand Privacy Act is a technologically neutral law with a concept-based strategy that makes it robust in the time of changing technology. Even decades later this strategy is not outdated. The existing legislation was not a robust one, and many other OECD states have modernised their data protection and privacy laws. Factors why other states updated their privacy laws is since the globe is now inextricably linked. As a result, the New Zealand Ministry of Justice has initiated privacy law transformation with an urgency. The amendments to the Privacy Act involve a greater authority for the Privacy Commissioner, compulsory reporting of breaches of privacy, higher penalties and new transgressions. The amendments are aimed at encouraging public and private sector institutions to recognise risks and deter detrimental situations (Corner, 2018)

It is debatable from the GDPR point of view that multi-national organisations are most likely to engage in global commerce or information-related proceedings in the EU, however other companies can never be unworried. Organisations that were not covered by the current laws may have less admiration of GDPR's privacy requirements than those already complying. For the considerations of obtaining discrete EU data, the European Data Protection Board has the powers to white-list nations beyond the EU; and New Zealand is already on the authorised list. Concerns about privacy related cross-border data transfer is currently addressed by New Zealand through the Privacy (Cross-border Information) Amendment Act 2010. According to this Act, on legitimate reasons, the

Commissioner may forbid the transference of personal details from New Zealand to some other State (Ingley & Wells, 2018).

New Zealand recently established a civil action on privacy interference. It included components like: (i) The presence of information with sensible expectations of privacy, and (ii) Promotion offered to certain confidential evidence which would be considered extremely objectionable to a reasonable intelligent individual. New Zealand's Privacy Commissioner regularly publishes indicative case notes related to information privacy law (Gunasekara & Toy, 2011).

2.10 IMPLEMENTATION ISSUES AND PROBLEMS

With a wide array of requisites to comply with the Regulation, the necessity to abide comes with its own issues and problems. Following are few of the issues and problems identified as part to the study.

Personal data security has several goals. The controller will be the only actor to carry out measures for technological and organisational protection. The processor has an implicit obligation with the controller based on an agreement. The Regulation requires both controllers and processors to take the necessary safeguards (Wolters, 2017). For instance, a data controller outsourcing its staff email services to a private entity wants the email service to provide essential features such as spam and malware filtering, but those features are useless unless the private entity can improve continuously by assessing email messages to determine new and emerging threats. Hence data security is a responsibility for both (Hintze, 2018).

The data subject's stance with respect to the controller is poor. Throughout the course of their professional practices, a controller usually processes personal data. In fact, several controllers process the personal information of a citizen in numerous other contexts. A data subject is virtually unable to keep an accurate account of these controllers and process activities. In addition, the precise ramifications of individual activities could be hard to determine. The citizen must not enjoy the authority of access unless the citizen knows the entities who may process the personal information or if the information supplied cannot be valued (Wolters, 2018).

In the case of a legal basis, 'Consent' has a significant meaning under the GDPR, which is different from the common English meaning, in which data collection is a condition for receiving any service. The ICO (Information Commissioner’s Office) asserts that if you require someone to accept processing as a business condition, it is not likely that consent will be the best suitable legal way for processing. Thus, the two most probable bases for processing personal data will usually be 'contract', or 'legitimate interest' in cases where there is no contract (Membrey & Mitchels, 2019). A grey area exists where online service providers could assume that children of certain age would be knowledgeable to provide their own consent for processing (Atkinson, 2018).

It will be daunting and costly to hunt for and hire DPOs (Data Protection Officers). Not only are organisations subject to the GDPR, they also must appoint a DPO – just their own employee or joint personnel, may be as their staff or outsourced to a freelancer. A DPO's responsibilities are diverse and can go well for the specific controller as well as have a problem (Daniela, MacGregor & Michal, 2018). The DPO may also perform other duties, provided that such duties and tasks do not give rise to conflicts of interest. Organisations should establish internal rules and provisions so that the DPO can remain independent and work without conflicts of interest (Cliza & Spataru-Negura, 2018).

GDPR entails an active (as opposed to passive) consent and a legitimate and tangible decision. Digital marketers know that internet service users theoretically accept the terms of service of all such companies when they register online. It does not indicate that users are ready to have their personal data collected throughout the digital, physical, on- and off-platform worlds and have that data used to establish a behavioral profile for digital marketing purposes. Operational ambiguity for digital marketers includes a restriction on computerised decision-making in the inexistence of a tangible consensus of the user, making it harder to validate compliance (Ghosh, 2018).

Lawmakers and regulatory authorities are forging a new attitude which states that data stockpiling by major organisations can become a barrier to innovation and competition. New services must have access to new customer information and data portability is a means of achieving this. In an environment where users could transfer their information from one controller to another, an innovative competitive aspect is created around the access to customer information. Critical information are no more the ones that organisations amass from their clients, but information that can be collected from other organisations. The difficulty is to create customer value from the data collected by organisations (Mitchell, 2016).

In Australia, there are compulsory data retention laws, having relentless state surveillance capabilities and an assortment of inexplicable power in the hands of a Minister of Home Affairs. The Australian Government is trying to challenge the encryption standards which reinforces all the financial transactions and private communications. Such laws are in loggerheads with the GDPR, where encryption is a recommended privacy enforcement mechanism (Ludlam, 2018). Another area of concern is portable storage devices, especially when left in the hands of staff not knowledgeable about GDPR. Ensuring encryption of such devices becomes a challenge to enforce compliance (Burns, 2018).

Civil liability may also result from the GDPR. Any person who has undergone an impact because of a GDPR violation shall be eligible to indemnification from the data processor or data controller. Companies need to evaluate their prevailing techniques and processes that address safeguarding of information and privacy, such as their IT policies, HR policies, outsourcing procedures and any policies that affect data subjects in the European Union. Therefore, appropriate policies should be tracked, analysed and shared to staff on an ongoing basis. (Mueller, 2017). As far as the fact is concerned, companies could call for sanctions by failing to wipe out the memory of redundant IT equipment before the disposal. A researcher also uncovered that employees did not know whom to contact to correctly dispose of outdated or unused equipment within their company (John, 2018).

Under international norms, a state is prohibited from carrying out an intervention in international territory if it comes inside the absolute abilities of authorities of foreign nations, for example data breach investigations. The foreign state's approval must always be obtained, irrespective of the foreign organisation’s consent. Coordination with international jurisdictions relies on the GDPR implementation beyond Europe to the degree that the demand is practical and genuine (Azzi, 2018).

Through the GDPR, an emphasis on people in the EU is replacing the significance of the location of the hardware (e.g. cloud storage overseas). The GDPR shall apply to the processing actions of an enterprise in the EU, irrespective of where the processing is carried out. In the event of a disagreement between EU Member States' national laws and other global regulations, which concerns not alone the EU but the world. A major issue is how the principle of territoriality would be implemented and whether it would undermine international law to prefer national law over international law (Bu-Pasha, 2017).

Data controller and data processor concepts can often be misinterpreted, and there is not always a clear distinction between them. The comparison of "data controller" with "data owner" is a major error. While data possession and data control sometimes correlate, they are distinct notions, and would not automatically ascertain the other. An entity can thus be a controller of data in relation to data that it does not own (Hintze, 2018).

Data controllers must place a policy on their online sites to educate the public of privacy risks, yet many customers would not understand them. Such disclosures are becoming longer and far more complicated due to the rapid development of technology. Although data subjects should have the choice of expressing consensus to processing of data, they almost always seem not to contemplate about the repercussions of consenting. Instead, they plainly consent to a request. In addition, policies are subject to frequent modifications and, so when this occurs, people must re-read them to understand about the impacts for their private information. It really gets much harder to take a knowledgeable decision about disclosure of personal data. GDPR is often criticised by the behavioral scientists for not addressing such threats involved with the control of consent by the data subjects (van Ooijen & Vrabec, 2019).

Article 20 of the GDPR does not make it clear if the information that the service provider produces for quantitative and logical determinations such as internet-based standings may or may not be subject to data portability. For instance, if an on-line seller decides to port from service provider A to service provider B, then the associated on-line feedback scores of the seller also needs to be ported. It would be important to see if data controllers will consider ways to exploit the regulations to deny transferring data to another controller and whether any eventual issues will be monitored to address them in the future. Also, the figures related to the costs involved in complying to portability requests have not been reported (Vanberg, 2018).

GDPR considers a greater scope for personal data now than before, creating greater cost and complexity. Even though the GDPR aims at more focused kinds of personal data, it extends its classification to also include less acquainted kinds, such as location data and online identification to more than one aspect explicit to that natural person's bodily, physiology, genomic, psychological, financial, public or societal distinctiveness. Also, it limits the processing of several varieties of private information, such as information disclosing ethnic or racial etymology, political-party affiliations, spiritual or cultural affiliations, or affiliation of employment unions, and different forms of medical information. They would not be useful if an employer needs such processing to deliver benefits schemes (Blair, 2018).

Research have revealed that understanding of privacy-improving techniques in medium and small-sized businesses (SMEs) is low while those who know are further likely to assume that the cost of realising them is overshadowed. So small and medium-sized enterprises could end up taking risks and just discount the Privacy by Design obligation of the GDPR. In the absence of real competitiveness between Privacy by Design techniques, there may be an opportunity for strong, established players in the market to organise alliances, approving financially advantageous Privacy by Design techniques that minimise regulatory restrictions on processing of data within the parameters to the extent necessary of a temperamental legal standard (Diver & Schafer, 2017).

The GDPR has not defined what is implied by the term data breach of the right to data protection, nor does it define the concept of damage. It specifies that the data subject shall only be entitled to file a suit if they consider that their right to data protection has been breached because of data processing in non-compliance to the GDPR requirements. Also, compensation is legally allowed to the data subject who has endured tangible or moral damage (Ungureanu, 2018).

It can now be observed that there is a shift from GDPR-specific anxieties to a wider acceptance that organisations will have to revise their current organisational strategy for data protection. Issues regarding constantly renewing data protection laws and their related compliance costs have become the biggest risks for organisations worldwide. A latest global survey by Gartner revealed that risks related to competent resource scarcity had been replaced by the risks related to constantly renewing data protection laws. With the GDPR in force, managers are now realising that compliance with data protection laws is more expensive and complicated than expected (Paredes, 2019).

Small businesses find it difficult to initiate privacy protection. It is not obvious to have the totally correct layer of security in place. Over and above the professional training of staff on privacy practices to be followed, the installation of firewalls and anti-virus software become a bare minimum requirement. Without proper security, an enterprise cannot have privacy. Information must be secure to stay confidential. The GDPR expects attention paid to everything that could identify anyone which includes information associated with respect to names, contact details, driver’s license number, website cookie data, and so on. The guidelines of the GDPR require substantial tiers of data security on information such as health or genetic data and biometrics (Bennett, 2018).

In complying to the GDPR, there seems to be an absence of ownership within an organisation. People argue that it is not their obligation, that GDPR compliance, training and communication are the responsibility of IT, human resources or any other department. Experts claim that many organisations acknowledge that although they have been told to do everything to prepare for and comply with the GDPR, they have not been given good assistance on precisely what needs to be done. Although organisations are better acquainted with the transitions that they need to make to their GDPR data management procedures and policies, not all are in a rush to get it all done (Ross, 2019). A general assumption for organisations outside the EU is that they are not covered by the GDPR plainly because they are not within the European Union. To conform with the GDPR, organisations bank on their IT department. Most of the requirements of the GDPR impact the way a company does its business. Compliance with GDPR is not just technological conformity. Few organisations think that all GDPR prerequisites will be met by a privacy notice and a consent check box (Cox, 2018).

2.11 CONCLUSION

Personal data has been used against the owners to jeopardise their identity and cause mayhem. It is evident that while global regulators understand the consequences of changing environments in computing systems, they will also change how data is managed in their countries. (King-Bailey, 2018). Compliance with GDPR is not a one-time task. It is a continuous process. The underlying fact is that, companies wishing to be successful in the European marketplace must ensure that they conform to the GDPR (Mueller, 2017).

The fundamental idea is that individuals must be able to manage their personal data, also called "informational self-determination". It indicates that people are entitled to ascertain when, how and for what intent personally identifiable information is being held and used about them. (Mueller, 2017). GDPR's ultimate future direction is based on how the three elements of people, process and technology combine to deliver the intended results. The need for such a regulatory control is apparent as medical equipment technology, pharmaceuticals, biologics as well as other international enterprises become more and more automated (King-Bailey, 2018).

The new legislation on data protection introduces several key changes for all segments of the population engaged in the private information processing. The aim is therefore to hold controllers of personal information accountable and to reinforce the rights of the citizen (Chirica, 2017). To ensure that data portability is enforced successfully, the reasons given by controllers of data for rebuttal to conform with portability of data appeals must be monitored and analysed. It is obligatory to ascertain the scope to which portability of data drives innovation, growth of the economy and consumer welfare, fulfilling the European Digital Economy promise (Vanberg, 2018).

Global organisations need to evaluate their business model, base of customers and activities to ascertain whether the GDPR is applicable to them. Though the GDPR does not extend to few organisations, there are quite a few data security and privacy practices to be aware of. Where applicable, ensure that cross-border transfer of data and compliance with GDPR are addressed and review the existing agreements with vendors and partners. Assess how much and what data is gathered, stored and shared. Compliance cannot be initiated until you know what data you have and how you use it. Organisations planning and tackling the challenge will have an edge over their rivals. GDPR may well transform the way business operates, but business will continue as with many previous changes (Cox, 2018).

Chapter 3
METHODOLOGY

3.0 INTRODUCTION

The General Data Protection Regulation (GDPR) shall be complied with by all organisations running operations with people situated in regions of Member States of the European Union (EU). Inability to comply with the legislation might have serious economic and judicial implications. In the case of failure to comply, the GDPR raises fines and other penalties. Based on the general management procedure of data, the preparedness evaluation starts with the identification of the information gathered, interpretation of how the information would be utilised, as well as the prospective threat of revelation or mishandling of the information (Bowen, 2018). The importance of privacy and data security has been acquired through the legislative, organisational, technical and leadership risk in the recent past. These risks are mostly divided from each other and, more importantly, from technical methods (Martin & Kung, 2018).

To safeguard their private information, the EU GDPR says that companies should implement suitable strategies, processes and mechanisms. The ISO 27000 suite is a collection of information security requirements that recommend proper protocol for information security governance. The GDPR does not safeguard all information, as it applies mostly to private information (Lopes et al., 2019). Through this case study it is intended to understand the possibility of implementing Privacy by Design through a combination of operational / management methods and Privacy Enhancing Technologies. The operational / management methods are planned to be achieved through the guidelines available from ISO 27001, IS0 31000 and BS 10012 standards. The ISO 27002 provides the guideline to implement technical controls at organisation level to ensure security. The same guidelines can be adopted to implement technical controls to safeguard privacy of the citizens. The intention of the case study is to implement pseudonymisation on the legacy data collected. The technical controls shall be implemented on the publicly available datasets. As part of the technical controls, it is intended to use the database management tools which are available in the market. Also, a software utility tool is intended to be developed which can be used to mask the data and achieve a similar result as that of the database management tool.

3.1 RELATED WORKS

Many businesses ignored the GDPR preparations up until the final moment. Most of them did not understand how to start and concentrated on the adverse effects of failure to adhere. High penalties, the unseen implications of future litigation, collapsing of customer trust and ruined brand equity all come immediately to the mind of CIOs, Data Protection Officers and executive-level managers facing GDPR transition oversight. Controlling the information collected and processed by the business would deliver not only compliance, but an entire range of other advantages as well. The GDPR could be an initial measure towards obtaining meaningful protection by pressing organisations to connect separate data storage systems and using tools more objectively against several forms of data. Doing so would allow companies to develop efficient tools to recognise patterns, accurately forecast operations, monitor technology and business variations and recognise fresh business potentials. Establishing a technical approach which is also rational regarding the information that a company governs is critical. Each regulatory issue addressed individually, results in reduced volumes of threats and penalties (Garber, 2018). The following studies performed on the compliance of GDPR through various methods enables me to understand the existing compliance strategies adopted.

3.1.1 Bowen (2018)

As medical service entities negotiate an incredibly complicated regulatory structure, managers encounter tremendous difficulties at different stages. These stages involve such as HIM (Health Information Management), Release of Information (ROI), conformance, financial resources, Health Information Technology (HIT), privacy, and security. As per the results of the Veritas 2017 GDPR Report, nearly one in three (31%) of the participants said that their company now complies with the main demands of the regulation. Though, when questioned regarding GDPR regulations for some of those participants, most of the responses demonstrated that they are doubtful they comply. Just 2 percent happened to have complied, showing a clear ambiguity about preparation to govern the regulation. Results indicated that just about half (48%) of companies that reported being conformant, do not even have complete awareness of events involving sensitive information infringement. In addition, 61% of the same sample acknowledged it was indeed hard for the company to recognise and publish infringements of sensitive information in less than 72 hours of realisation. Every entity who is unable to communicate sensitive information infringement to the supervisory authority in that period breaks the regulation’s important criterion (Bowen, 2018).

A paper published in 2017 by the International Association of Privacy Professionals (IAPP) offers an assessment of commonalities and dissimilarities in criteria for the compilation, usage and safekeeping of HIPAA private information and the management of medical data as confidential private information under the GDPR. The GDPR encompasses all private information, including information outside of the reach of HIPAA, as per the paper. The health data of the GDPR is comparable to the Protected Health Information (PHI) of HIPAA. Even as HIPAA regulations primarily extend to implied organisations and their corporate partners, the GDPR specifications affect non-EU organisations as well. Entities in the EU and the U.S. that use and process or publish PHI thus need to have a complete knowledge of the appropriate information constraints. The ‘consent’ for the use or publication of PHI is a significant scope of evaluation is discussed by the IAPP. An organisation or business should always specify the planned objective for the usage of that private data acquired in the EU (Bowen, 2018).

The following measures are suggestions to qualify for GDPR privacy and security demands from both U.S. and EU entities and companies. 1) Enhance understanding. Ensure that all interested parties and management are conscious of the modifications in GDPR information privacy legislation and how they contrast with HIPAA regulations. In order to comply, effective readiness is crucial. 2) Entire information must be recorded. It involves the complete collection and maintenance of PHI, such as, information’s usage, accessing information, processing, sharing and transferring information. Encompass data management principles such as responsibility, clarity, security, accessibility, storage and disposal. 3) Examine of present privacy notifications. Consider every modification which could affect the privacy notifications and share such data throughout the organisation. 4) Verify the rights of individuals. Make sure that the processes address all personal rights, such as how to erase private information or digitally offer information in a widely utilised structure. Among the most important amendments is indeed the right to be forgotten, that necessitates the capabilities to recognise and delete data of a person. 5) The policies related to consent must be evaluated. Contemplate minimum provisions for verifying the age of people and obtaining approval from parents or guardians for every kind of information handling activity. 6) Evaluate processes for infringement of information. Regular risk assessments must be carried out to assist avoid infringements. Examine potential risk domains that might be cues for GDPR specifications. 7) Identify an officer for data protection. Such an individual is accountable for adherence with privacy protection and plays a main role in the establishment and enforcement of information management procedures (Bowen, 2018).

3.1.2 Lopes, Guarda & Oliveira (2019)

The ISO 27001 standard is the global structure for managing the security of information. In the course of time, the ISO 27001 standard has been continually improved and derives out of a prior set of norms. ISO 27001:2013 is component of an organisation's leadership scheme focused on a risk-based strategy which is designed to develop, execute, function, monitor, retain and enhance information security. ISO 27001 describes three key elements or components of efficient protection of data: people, process and technology. Such a three-dimensional strategy enables organisations to protect themselves against several structured and prevalent inner challenges, including inadvertent revelations and human factor mistakes (Lopes et al., 2019).

The subsequent benefits that organisations gain due to the application of an information security management scheme in accordance with ISO 27001 are as follows (from the Standard). It allows risks and security flaws to be identified and eliminated. It gives all participants (customers, associates and others) information protection and assurance. It enhances knowledge of information protection. It improves the ability to anticipate, handle and withstand a crisis. It strengthens the company's understanding related to procedures, resources and responsibilities. It offers true understanding of the threat faced by the organisation. It guarantees continuity of service. It decreases expenditure and enhances the current practices and operations. It guarantees adherence to existing regulations. Adoption of ISO 27001 means a strong obligation to data security (Lopes et al., 2019).

The resemblance between the ISO 27001 structure and the GDPR specifications imply that organisations conforming to the specification also comply midway with GDPR. ISO 27001 specifications are comparable to the GDPR in several areas. Though the legislation briefly indicates methods (such as involving cryptography), ISO 27001 also sets out what organisations must do to stay vigilant. Article 42 of the GDPR provides information of adherence with the Regulation by means of certification procedures for protection of data (Lopes et al., 2019).

When organisations have an effective ISO 27001 structure, they cut administrative overhead, time and expenses to meet GDPR demands. If an organisation is not accredited in accordance with ISO 27001, the GDPR implementation gives strong protection of information. ISO 27001 does not effectively address some of the GDPR criteria; but, ISO 27001 offers the resources to move businesses to a level nearer to achieving compliance with the legislation. In contrast to the GDPR, ISO 27001 would not specifically address the following data security challenges: 1) Consent, 2) Portability of information, 3) The right to erasure, 4) The right to the processing restriction, 5) Right to oppose, and 6) Global transference of private information (Lopes et al., 2019).

The contents of 15 websites were evaluated and analysed by examining if the application of ISO 27001 could facilitate the compliance of GDPR in organisations. It was discovered that 60 percent of websites agree with the assertion that the application of ISO 27001 treats private information as a data security asset and that there was no reference of any kind in the other 40 percent. It was identified that to be compliant with GDPR, three key aspects were required: 1) Certification, 2) People, Process and Technology, and 3) Controls and security frameworks. It was discovered that the aspects of consent and penalties stood out and are comprehensive in the GDPR but hardly mentioned in ISO 27001. 73 percent accept that the ISO 27001 specification was an outstanding structure for adherence with the EU GDPR and 20 percent dispute this element. Out of these results, it could be observed that while ISO 27001 would not include specific significant provisions, its application is regarded as an enabling mechanism for organisations to meet the current regulations on personal information (Lopes et al., 2019).

3.1.3 Kammueller (2018)

The Isabelle framework is described for the examination of infrastructure privacy and security by using policies. The whole framework was originally developed for internal threat simulation and evaluation. The use of it was affirmed on the most familiar schematics of internal threats recognised by the CERT-Guide for Insider Threats. The Isabelle framework was implemented effectively on practical cases for aircraft safety, including insider attacks and bidding procedures. The Isabelle framework was revamped in the course of the study so that it is currently a common context for the government-backed infrastructure assessment of security along with its principles and stakeholders. It was verified through demonstration that it was possible to use the Isabelle Infrastructure framework for compliance monitoring of the GDPR. By the usage of Kripke framework and the Computational Tree Logic (CTL), it has described how the Isabelle Infrastructure model could officially modulate the technical criteria contained in the GDPR. It demonstrated how to encode the architecture of the system and define privacy access control on a healthcare IoT system for observing the patients (Kammueller, 2018).

3.1.4 Elluri & Joshi (2018)

As the GDPR legislation is presently accessible in the form of text, substantial human and time-consuming efforts will be required to comply with it. The study utilised the Web Ontology Language (OWL) of the Semantic Web technology to produce a graphically represented policy oriented knowledge-base about the GDPR legislation. The GDPR laws had been categorised as requirements for controllers and processors in the graphical knowledge-base. The relevant Cloud Security Alliance (CSA) mechanisms was also incorporated with these requirements. The GDPR legislative records were studied and found that only the articles mentioned below influence the processors of cloud services and the controllers in relation to a total of 99 articles (Elluri & Joshi, 2018).

Cloud controller requirements: Article 5 – Processing of personal data – Which infers that private information with reference to the data subject should be processed legally, reasonably and transparently. Information shall be obtained for a reason and the processing must not be done in a manner inconsistent with that reason. Article 24 – Controller responsibility– Illustrates that the controller shall be liable for the implementation of any technological or operational measures necessary to comply with GDPR. Article 25 – Information protection by design and by default – It involves the organisation to obtain, retain or information processing for the necessary reasons only through the application of methods such as pseudonymisation and information minimisation. Article 26 – Joint controllers – This article requires all of them to be compliant with GDPR irrespective of whether there is more than one controller. Article 27 – Delegates representing the processors and controllers not based in the Union - A delegate who is a legitimate or constitutional person located in the EU should be appointed if the processor or controller is situated beyond the EU. Article 34 – Notification of private information infringement – The data subjects must be notified in a simple and straightforward language about any of the data breach that could influence their freedoms and rights (Elluri & Joshi, 2018).

Cloud processor requirements: Article 28 (2-4) (10) – The processor’s responsibility – The processor shall decide on privacy responsibilities and comply with the regulations for the selection of sub-processors. Article 29 – Processing under the controller’s discretion – The processor shall process the information according to the directions of the controller, except if asked by the Member State law or the Union. Article 37 – Designation Data Protection Officer – When it includes constant tracking of the information subject on a widespread manner, it is advised to employ a Data Protection Officer. It also states that the DPOs can only be recruited based on the practical specialist knowledge of privacy regulations. Article 44 – General principles for transfer – Data suppliers would be subject to trans-border data movement guidelines (Elluri & Joshi, 2018).

3.1.5 Martin & Kung (2018)

Laws and regulations for protection of data have existed for years and have developed alongside technology and society. Legislation and policies also require technicians to adhere to Privacy by Design (PbD) concepts and implement security and privacy alternatives all through their activities. They usually would work with, for example, dataflow designs, database systems or software implementation workflows under consideration. For the activities they handle, they almost always neglect interpreting legislative problems into functional tasks and operations. They seem to be doubtful about what the GDPR corresponds into the list of tasks and activities. The strategy for data security and privacy can be implemented if the practices of secure software development for dealing with certain types of specifications are followed for a considerable period. These concerns are answered whilst also maintaining the conventional techniques and mechanisms that are used by the professionals in their regular activities. To comply with the regulatory structure, professionals ought to have theoretical and technical capabilities to enable data security concepts to be applied systematically (Martin & Kung, 2018).

According to the European Data Protection Supervisor (EDPS), European Network and Information Security Agency (ENISA), and the PbD promoters, a meticulous solution creation and implementation of data security-oriented alternatives across platforms and procedures of software development was commonly acknowledged as the feasible solution to PbD. The backbone of this industry is in the techniques used by professionals to identify and solve concerns about data security throughout the various phases of implementation. Even though backed by teams of experts, it is argued that not every professional must be a specialist in data security, they would still confront problems of data security in their daily activities. By adopting standardisation through a high level of maturity in the practices and procedures enables the implementation and application of data protection techniques across a wide variety of software development activities. To ensure data security through privacy engineering, professionals must be trained at various stages of software development such as: the elicitation of requirements, analysis of software, design phase, data visualisation, verification, testing, and so on. It is necessary that security and privacy components are deeply integrated into user-friendly applications and programming tools by the developers. Also, the integration of data security and privacy operations into the various phases of the SDLC (Software Development Life Cycle) is also required (Martin & Kung, 2018).

The adverse impact of an unpredictable occurrence that digresses from the anticipated outcomes is termed a risk. Risk management promotes engineering-based implementation of Privacy Impact Assessments (PIA), consistent with the legal specifications of GDPR. Risk management begins with the classifications of personal information collected and the processing operations to whom they are susceptible. Possible threats are listed, and losses are assessed based on various variables affecting their probability of occurrence and effects. Risks are assessed, given priority and various measures are adopted, such as implementing relevant technologies or identifying mitigation alternatives. Eventually, there must be documentation and monitoring of risks. One of the approaches for data protection risk assessment is Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance (LINDDUN), that employs data flow diagrams (DFDs) to project the movement of private information all through the operations involved in processing and the controllers and processors' domains (Martin & Kung, 2018).

Under software engineering, there are functional and non-functional requirements that would be elicited during the initial stages of the project execution. The system requirements are collated under functional requirements and security and privacy requirements are collated under non-functional requirements. The inception of data security and privacy requirements seem to be clear. Firstly, the standards and regulations lay down processes, instructions and policies. Secondly, privacy objectives define the privacy characteristics that must be maintained. During requirements elicitation, techniques such as PROPAN (Problem-based Privacy Analysis) suggest the use of 'problem frames', which shall consider the system circumstances under evaluation. In terms of managing privacy demands, the commissioning of superior privacy objectives and data protection laws into privacy checks is an appropriate strategy. Such an objective-driven method complements risk management and promotes the suitable selection of alternatives (Martin & Kung, 2018).

A cycle of development progresses across various models. The model-based design approach enables the analysing and designing of systems for development. Primarily, out of a privacy outlook, an appropriate system model includes mapping of data and logging of the private information components to be processed by the system. Fundamental frameworks can generally be enhanced with details about the types of private data represented and appropriate data protection characteristics. In addition, the fundamental frameworks enable the comprehensive assessment and analysis of the design approaches and the decisions best suited to security and data privacy. Furthermore, automated Model-Based Testing (MBT) may be specifically applicable to verifying the right implementation of user access-control systems for private information. Finally, the assurance method promotes proof of adherence with the regulation and compliance with the accountability criterion by systematically capturing the facts, their relationship with artefacts and specifications, back trace to the regulation, and conformance reasoning extracted from those facts. Accreditation systems for privacy protection could also reap the benefits of the facts gathered (Martin & Kung, 2018).

3.1.6 Diamantopoulou, Androutsopoulou, Gritzalis & Charalabidis (2013)

Several researchers have studied the privacy specifications that must be used to maintain the privacy of individuals. While the benefits and possibilities offered by crowd-sourcing to policy-makers, the gathering of information, views and thoughts often poses a threat to the privacy of respondents in such material. In order to close the gaps identified in the study, an analysis was provided to fix the shortcomings related to privacy. It was carried out in three steps, via crowd-sourcing actively, crowd-sourcing passively and expert-sourcing passively. Crowdsourcing is the simplest method to collect enormous information on anything which could be used to supervise groups with higher risk without substantial manpower or infrastructural investment. By using a crowdsourcing method, private information and sensitive personal information can be collected on delicate problems. Crowdsourcing enables individuals to interconnect with each other, authorities to communicate for different events with the collective population. E.g. coordinating emergency relief activities, modelling political disputes, thus gaining data in a brief period, being closer to actual problems affecting individuals' daily lives (Diamantopoulou et al., 2013).

According to the spatial crowdsourcing classification, it refers to a visionary framework that involves groups of people, organisations or societies and intends to collect, analyse and disseminate environmental, interpersonal or other time continuum data. E.g. people could use their handsets to complete a task at suitable locations of importance. Severe consequences of privacy infringements might occur if an untrusted server is used and the specific places, their actions, the moment and location when they were connected to the site, and lastly, the location's characteristics, may be revealed. (Diamantopoulou et al., 2013).

The private-sector crowdsourcing has encouraged government institutions to develop public citizen-sourcing techniques. Governments are largely utilising ICT (Information and Communication Technologies), primarily social media platforms, to gather citizens' data, expertise, suggestions and views on major societal issues. Many of these ICT-related projects used 'active citizen-sourcing', that was based on using the social networking sites reports of state organisations to address a societal issue or policy. It required appropriate data, expertise, and thoughts and views from the population at large. A new strategy to citizen-sourcing by government has lately begun to be established, relying on 'passive citizen-sourcing'. Governments have a far more passive position in this strategy as they harness policies-related substance that has so far been openly produced by people, with no visible public assistance or guidance through multiple external social networking sites that do not belong to state organisations (Diamantopoulou et al., 2013).

During a latest conference on Privacy Engineering Research and the GDPR, it was stated that a variety of studies on Privacy Enhancing Technologies (PETs) has been already completed. Such techniques are essential and could be the foundation for any software engineering project and could be used efficiently throughout the execution stages. The major task at present is not to create varying PETs, but instead to function effectively with current methods that are already universally accepted. These techniques also enable data privacy professionals to seek a solution to promote Privacy by Design (PbD) and Privacy by Default specifications, by concentrating on providing effective data protection process patterns. As described in the earlier chapter, the basic privacy criteria are as follows: 1) Authentication, 2) Authorisation, 3) Anonymity, 4) Pseudonymity, 5) Unlinkability, 6) Undetectability, and 7) Unobservability (Diamantopoulou et al., 2013).

PETs are strategies designed to help people and organisations safeguard their privacy. They could therefore be classified into the following primary classifications: 1) management tools, 2) software tools, 3) anonymiser solutions, 4) systems and designs, 5) pseudonymiser tools, 6) Tracking and evidence removers, and 7) encryption tools. Every classification comprises certain technical application methods which, alongside interested parties and / or the software development team of the organisation, can be used as a rationale for the software architect to determine and suggest the most suitable methods which fulfil the data protection specifications described. Through adopting the appropriate data protection method to the corresponding data protection criteria, the recognition of a suitable PET will result in effective implementation (Diamantopoulou et al., 2013).

The methods that better serve and enforce the anonymity criterion are as follows. Products, systems and applications for anonymisers such as browsing pseudonyms, virtual email addresses, trusted-third parties, crowds, onion routing, DC-nets, mix-nets (Mix Zone), hordes, GAP, Tor, aggregation gateway and dynamic location granularity. Tracking and evidence removers such as spyware detection and removal, hard disk data eraser, user data confinement patterns and use of dummies (Diamantopoulou et al., 2013).

The methods that can be used to fulfil the unlinkabililty criterion are as follows. Products, systems and applications for anonymisers such as trusted-third parties, surrogate keys, onion routing, DC-nets, mix-nets, hordes, GAP, Tor and aggregation gateway. Pseudonymiser tools such as CRM personalisation and application data management. Tracking and evidence removers such as spyware detection and removal, browser cleaning tools, activity traces eraser, hard disk data eraser, use of dummies and identity federation that do not track patterns (Diamantopoulou et al., 2013).

The methods that can be used to fulfil the undetectability criterion are as follows. Management tools such as permission management and smart cards. Software mechanisms such as auditing and monitoring mechanisms. Products, systems and applications for anonymisers such as hordes, GAP and Tor. Tracking and evidence removers such as spyware detection and removal, browser cleaning tools, activity traces eraser, hard disk data eraser and identity federation that do not track patterns. Encryption tools such as encrypting email, encrypting transactions and encrypting documents (Diamantopoulou et al., 2013).

The methods that better help and enforce the unobservability criterion are as follows. Management tools such as permission management and smart cards. Products, systems and applications for anonymisers such as hordes, GAP and Tor. Tracking and evidence removers such as Spyware detection and removal, hard disk data eraser and identity federation do not track pattern (Diamantopoulou et al., 2013).

3.2 RELEVANT QUESTION DERIVED FROM ISSUES AND PROBLEMS

From the literature review performed in the Chapter 2, it is evident that to achieve compliance towards GDPR, a wide variety of issues and problems still exist. To comply with the regulation, there are numerous stakeholders who are responsible to perform specific duties to ensure adherence. Organisations must review their activities and determine whether they classify as a processor of data, controller of data, or both. Based on the nature of data collected, organisations must implement certain managerial and technical mechanisms to ensure privacy and security of the gathered information by them. If there are personal information collected or processed, then a consent must be sought from the citizens to proceed with the gathering and processing of information.

Based on the consent received, the collecting of information and processing might continue as per the requirements of the regulations. An inherent responsibility of the organisations as per the regulation is that at any given point of time such data must be traced back to the responsible individual. To ensure privacy and security of the information, technical measures must be put in place. The challenge here is that, such measures must be followed by implementing Privacy by Design approach. The approaches adopted must be universally followed by all departments within an organisation. This may include the operational department or the technical department of the organisation.

The complications involved in the compliance for GDPR puts the onus on Data Protection Officer (DPO) identified by the organisation. All the privacy related tasks must be reviewed and approved by the DPO. This also involves the identification of suitable training and awareness programs directed towards the staff members within an organisation. Increased awareness among the staff members is a key aspect in achieving the compliance. Organisations may look towards various industry standards such as ISO 27001, IS0 31000 and BS 10012 to ensure compliance towards GDPR through a formal certification. These certification programs allow organisations to adopt a uniformly laid down process to adhere to specific requirements of the regulation.

The following case study research question identifies the problem faced by organisations in the wake of GDPR and applicable to data that were collected retrospectively.

Research question (RQ)

How are the legacy data-sets collected by an organisation made to comply with GDPR? Accordingly, the case study objective of this thesis is to identify the possible methods to secure the data collected by an organisation to comply with the GDPR.

3.3 CASE STUDY SEGMENTS

The case study performed is segmented in to two paths. One, the operational / management path, and second, the technical path. From the literature review and the related works with respect to GDPR, it is observed that the compliance to the regulation can be achieved by adopting both industry standards and technical measures.

From the operational / management perspective, to achieve the GDPR compliance, the industry standards such as ISO 27001, IS0 31000 and BS 10012 were combined in order to arrive at the wanted requirements. These standards form an enabling platform to implement GDPR requirements within an organisation. These standards ensure that the organisation's business objectives are achieved while also complying with the regulation. Organisations do not have an option to stay out of complying with the regulation as there are severe penalties if any breach of data is reported. The penalties would not only add financial burden to the organisation, but also impact the goodwill stature of the organisation in the business environment. These standards actively enable organisations to assure information security by default. The effective employment of the standards could be achieved only through dedicated enforcement by the senior management. Through these standards, an organisation could meet the requirements for as information asset classification, privacy impact assessment (risk assessment), training and awareness, data collection and retention processes and the technical framework to confirm that the gathered information is secure.

From the technical perspective, the GDPR requires Privacy by Design and by default to be applied in all the information collection and processing phases within an organisation. This shall apply to both the controllers of the information and the processors of the information. Privacy Enhancing Technologies (PETs) enable Privacy by Design attainment. Once such technique is pseudonymisation. By applying a pseudonymisation technique, organisations can secure the information collected. It would ensure that the impact from a data breach, if any, would not lead to the consequent breach in the privacy of a citizen. By implementing pseudonymisation, the actual information is masked with random data which cannot be linked to the personally identifiable attributes of a data subject. Organisations need to adopt these technical measures as a default criterion while handling any private data of the citizens. To apply pseudonymisation, the operational / management standards form the basis by identifying the specific information that needs data masking.

3.4 THE CASE STUDY DESIGN

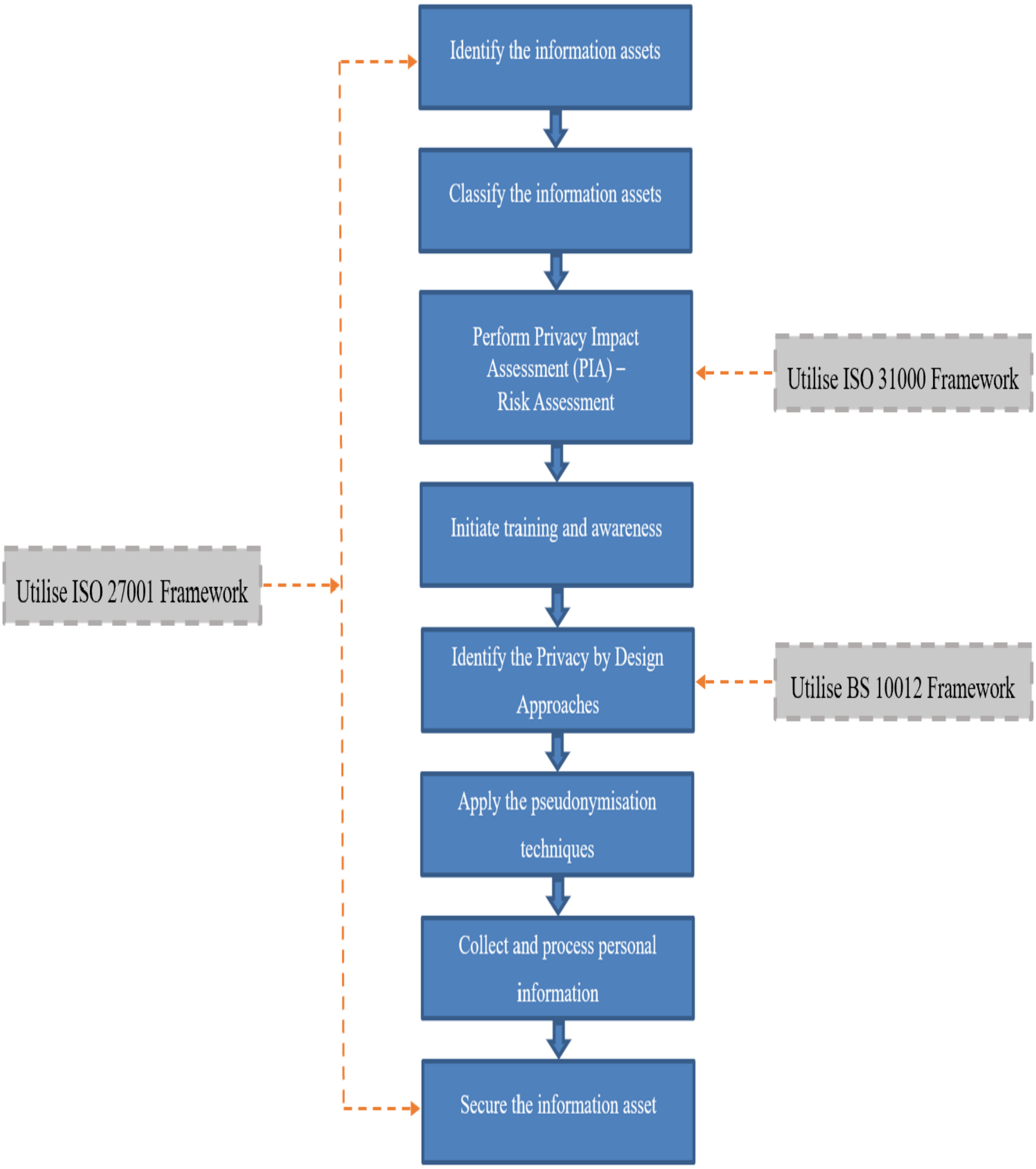

Identify the information assets
Classify the information assets
Perform Privacy Impact Assessment (PIA) – Risk Assessment
Utilise ISO 31000 Framework
Initiate training and awareness
Utilise ISO 27001 Framework
Identify the Privacy by Design Approaches
Utilise BS 10012 Framework
Apply the pseudonymisation techniques
Collect and process personal information
Secure the information asset

Figure 3.4.1: Case study design

As projected in Figure 3.4.1, the flowchart describes the various stages involved in the case study. The case study design approach adopts the best practices of ISO 27001, IS0 31000 and BS 10012 standards guidelines. The case study is initiated by identifying the information / data assets that would come under the ambit of GDPR as not all information / data assets would be requiring the enforcement of privacy guidelines. Based on the assets identified, they must be classified as an information asset that is generated within the organisation or that is provided by third-party sources to the organisation. The information classification allows the implement the appropriate privacy enhancing technology or mechanism to safeguard the data. Next, the privacy impact assessment is performed based on the determination of the information classified. This is achieved by performing the assessment of the risks related to the information assets that the organisation handles. Following the assessment, a comprehensive training and awareness program must be initiated within the organisation to sensitise the staff members of the risks and actions to be performed while handling personal information of any sort. Subsequently the Privacy by Design approach use to enforce privacy enhancing techniques must be evaluated and identified. Followed by the data collection and processing as per the identified pseudonymisation technique. By following these measures, the case study enables identification of the methods that can be adopted to cleanse the legacy data-sets collected by an organisation to comply with GDPR.

3.5 DATA REQUIREMENTS AND ANALYSIS

For the purpose of the case study, two publicly available data-sets were considered. The data sets identified were such that it had some sort of personal information. This assumed the fact that personal information was not secured in legacy data-sets. The data sets are then imported to a database management tool. The database management tool used for the case study is Microsoft SQL Server Express. The database management tool has built-in encryption syntax that allows masking the data by making use of an AES-256 encryption key. The encryption technique adopted is symmetric key encryption. The tool ensures that associated encryption key and certificate are generated to execute the encryption and decryption process (Refer figure 3.5.1.1). To ensure that there is no data loss in the due process, a random value is decrypted to check the integrity of the encrypted value. Also, as part of the case study, a GUI based software utility tool is developed (Refer figure 3.5.2.1). This tool can be used to mask the data to enforce pseudonymisation irrespective to any organisation or entity who work extensively on MS excel based data without using any commercially available data management tools. The output from the software utility tool can be used in conjunction with the database management tool as well.

3.5.1 Design for the database management based pseudonymisation tool

To implement the pseudonymisation technique, the first approach adopted will be by using the database management tool. The tool used here is the Microsoft SQL Server Express. Following is the design approach for the data masking of the legacy data set.

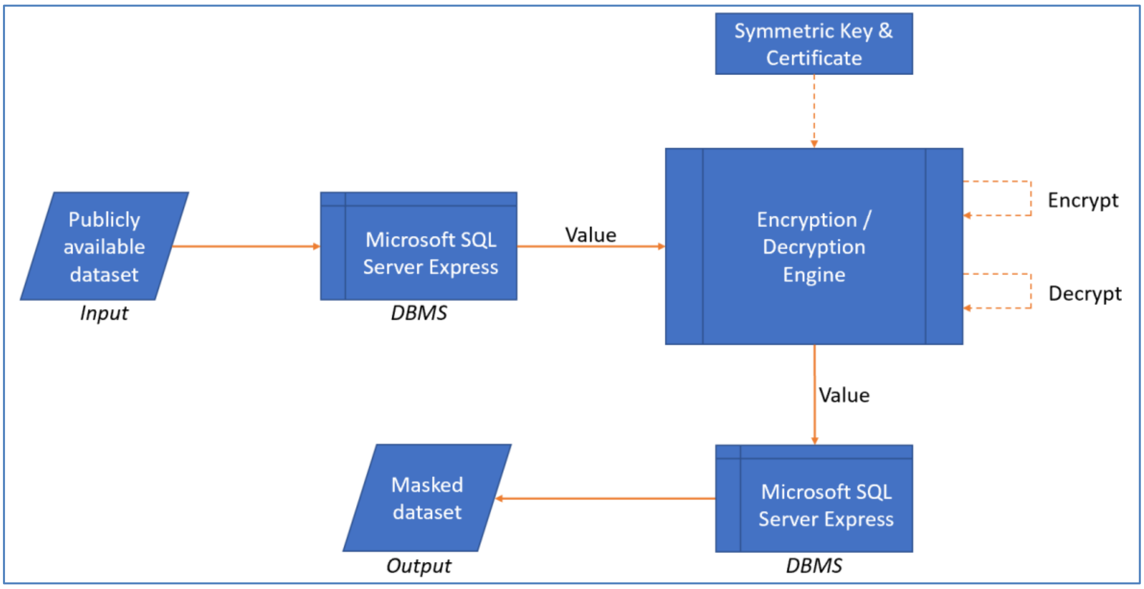

Symmetric Key & Certificate
Publicly available dataset
Input
Microsoft SQL Server Express
DBMS
Value
Encryption / Decryption Engine
Encrypt
Decrypt
Value
Masked dataset
Output
Microsoft SQL Server Express
DBMS

Figure 3.5.1.1: Data-flow in the database management based pseudonymisation tool

The algorithm for the database management based pseudonymisation tool is as follows:

Algorithm 1: To encrypt the values loaded in to the database management system

Input: A publicly available dataset will be sourced from online sources for the demonstration purpose

Output: The identified datasets will be loaded to the Microsoft SQL Server Express database management system. Using the built-in syntaxes, the below algorithm is drafted:

i) A master encryption key will be created

ii) A certificate will be created

iii) A symmetric key with AES 256 encryption by using the certificate is created

iv) Based on the privacy impact assessment performed, the necessary columns containing personal information will be encrypted

v) For demonstration purpose, the actual value and the encrypted value will be displayed side by side in the database management tool

Algorithm 2: To randomly check the integrity of the decrypted values in the database management system that was encrypted using the previous algorithm

Input: Encrypted values of the dataset in the database management system

Output: The identified values from the dataset will be decrypted using the built-in syntaxes, the below algorithm is drafted:

i) State the column with encrypted value (The encrypted value is 256 bits)

ii) Decryption will be performed by the symmetric key using the certificate

iii) For demonstration purpose, the actual value, encrypted value and the decrypted value will be displayed side by side in the database management tool. The actual value and the decrypted value must be same to verify the integrity of the output

3.5.2 Design for the GUI based pseudonymisation tool

The implementation of the GUI based pseudonymisation tool will be done using a combinational approach based on Protecting The CDN Application Files From Unauthorised Requests (Ghanbari, 2015), Getting started with Steganography (hide information) on Images with C# (Delgado, 2017) and RNGCryptoServiceProvider (2015). Following is the design approach for the data masking of the legacy data set.

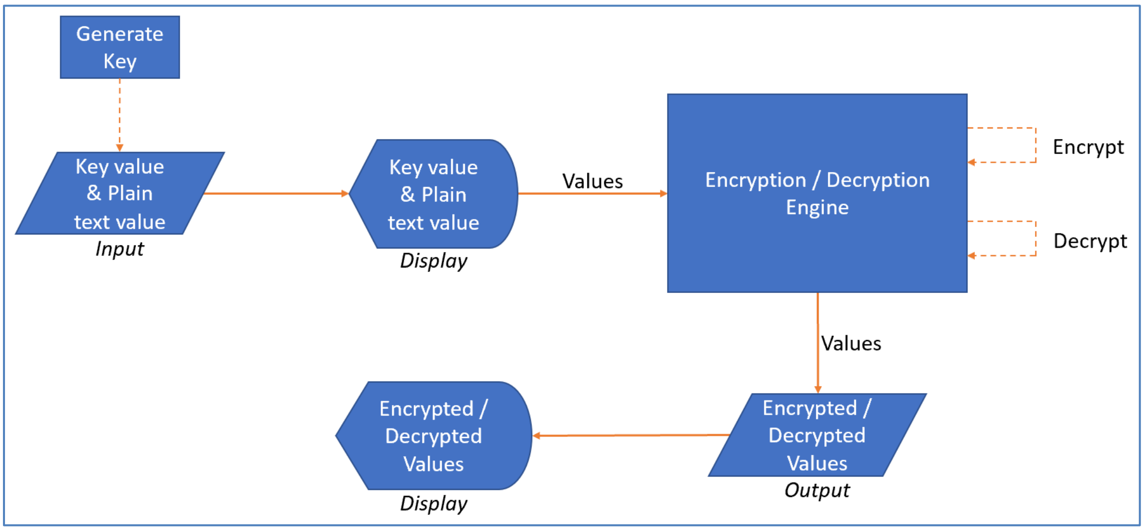

Generate Key
Key value & Plain text value
Input
Key value & Plain text value
Display
Values
Encryption / Decryption Engine
Encrypt
Decrypt
Values
Encrypted / Decrypted Values
Output
Encrypted / Decrypted Values
Display

Figure 3.5.2.1: Data-flow in the GUI based pseudonymisation tool

The algorithm for the database management based pseudonymisation tool is as follows:

Input: A randomly generated key and the plain text is entered in the GUI tool

Output: The encrypted values will be displayed in the GUI tool

i) The key size must be entered

ii) Using the key size, a random key is generated based on an array of characters which includes alphabet, numbers and special characters

iii) Encryption process is performed using salt strings, IV strings and plain text. The plain text is encoded using UTF-8

iv) Use PKCS7 for certificate generation along with the symmetric key

v) Generate the encrypted value which contains 32 Salt bytes, 32 IV bytes and 64 Cyphertext bytes

vi) To decrypt, repeat the steps in reverse order

vii) For demonstration purpose, decrypt a random value using the same key. The actual value and the decrypted value must be same to verify the integrity of the output

3.6 LIMITATIONS OF THE METHOD

Securing personal data of individuals in an organisation which is involved in controlling and processing of the data has changed. The case study performed here has its limitation from the implementation of privacy measures within an organisation. These limitations can be attributable to the privacy-aware culture within an organisation which is based on the best practices observed in the industry and the tools and techniques available to the organisation in securing the data it has collected and maintained over the years.

The limitations related to privacy-aware culture begins from the ambiguity in implementing the management standards. As there are multiple standards available, it becomes an overhead to maintain certifications to comply with the respective standards and therefore resulting in a weaker GDPR compliance by organisations. The implementation of these standards is hindered from the certification costs involved. The costs involved could be such as to hire a dedicated staff and department overlooking privacy and security. Few may argue that it is possible to conform to the GDPR by assuring and employing all the technical methods required within an organisation. The side-lining of the implementation of the management standards are also due to the requirement of heavy documentation evidences. But the human factor involved in the implementation of privacy related controls would not be inspected and corrected without a dedicated unit within the organisation.

For small and mid-sized organisations, it would be effective to use the database management tools such as the Microsoft SQL Server Express as it provides enough free resources, but, limiting the full usage of the database management tool. The database engine can use only 1 GB of memory at most and the size of the database is restricted to 10 GB. Automation of some of the intended tasks are not possible as the SQLAgent is not available. This impedes the automation activities such as job scheduling, database monitoring, data back-up, and so on. Scaling up of performance becomes an issue over a period when the number of users accessing the database increases. These limitations are also attributed to the costs that organisations can consider while implementing privacy related controls. The cost of acquiring a full version of the database management tool drives away the smaller organisations from implementing privacy related controls at database level in their daily tasks. As part of the case study, basic security is ensured by using the Microsoft SQL Server Express and the GUI based software utility tool. These have not yet been validated against brute force attacks or malicious attacks.

3.7 CONCLUSION

Though increasingly private, confidential and sensitive data are captured, communicated and maintained digitally, it is anticipated that suitable steps are being taken by people and organisations to guarantee the privacy of these kinds of data. In addition, it is crucial for people and organisations to recognise the elevated significance of every other set of data they disclose throughout their communication with services on the internet, as well as the risks that such disclosure may conceal. Privacy is not just a simple strategy, as privacy is a multidimensional notion with different variables to be considered on the technological and societal scales. The GDPR defines that one of the responsibilities of data controllers is to take suitable technological and operational steps to enforce information security by design and by default in the digital facilities offered to people (Diamantopoulou et al., 2013).

The current data privacy legislation presents a group of regulations requiring organisations to bring in controls. ISO 27001 can be implemented to assist organisations meet these demands. The GDPR promotes the employment of accreditation like ISO 27001 to demonstrate that organisations manage its information security efficiently in accordance with global best practices. Results have enabled to conclude that if any organisation which has already introduced ISO 27001 or was in the processes of applying it, then it is in an outstanding place to demonstrate adherence with the new GDPR specifications (Lopes et al., 2019).

The case study method provides an elaborate plan to execute the research in implementing operational / management methods and technical controls to comply with the GDPR. Previous works have revealed few of the outcomes that have been implemented and how the privacy issues were addressed. Also, previous works did reveal few of the short comings of the research that they had performed. By adopting Privacy by Design, the methodology for this case study intends to implement both managerial and technical controls to address privacy and security in organisations. As the awareness of privacy breach implications are well known, the latest data collection and processing mechanisms have been designed in such a way that it addresses the privacy related aspects at all stages. But for organisations which have abundant legacy data sets not compliant to the GDPR, it makes the adherence an achievable but difficult task. By implementing these controls, it enables organisations to achieve their business goal and objectives and as well as address the requirements to meet the GDPR specifications.

Chapter 4
CASE REPORT

4.0 INTRODUCTION

As described in the Chapter 3, the case study is designed based on the best practices available in the industry. One such standard is the ISO 31000 which enables to adopt the specifications required for risk management. In the sections below the list of risks are identified that would impact the privacy related aspects in an organisation.

4.1 PERFORM PRIVACY IMPACT ASSESSMENT – RISK ASSESSMENT

Processing operations are inclined to pose a substantial risk to the individual's entitlements and liberties. Hence, the impact assessment of information security must be undertaken by the processor and the controller to analyse the source, type, specificity and intensity of the risk. The impact assessment must comprise the actions, provisions and methods envisioned to mitigate such a risk, facilitating the security of personal information. It is during the initial phase of the project; an information security risk assessment is carried out to define the required security controls.

Following are the probable list of privacy related risks that an organisation may come across:

1) Lack of security awareness in employees may compromise the sensitive data. Due to the lack of awareness, security controls/processes laid down will not yield the intended results and loss of data
2) Lack of effective disciplinary process may lead to repetition of infringements of security. It might lead to the theft, losing business reputation and loss of data
3) If the assets are not listed, some assets may be missed which could be manipulated or be misused and can lead to unauthorised use of the asset and loss of asset
4) Inadequate classification of information may lead to inadvertent leak of confidential information
5) Incorrect / lack of labelling of information may cause the leak of sensitive information
6) If there are no restrictions on usage of USB and other removable media devices in the organisation, there is a possibility of replication and misusing sensitive data

7) If secret authentication information is shared / leaked it can cause issues due to unauthorised access such as misuse of system, integrity and loss of confidentiality
8) If access rights are not adjusted or removed as required it could lead to unauthorised persons having access to the systems or authorised persons not having access to required systems
9) If user’s secret authentication information is shared or seen, it could lead to misuse of systems and leak of confidential information
10) If physical locks are not available for all movable devices like laptops, it may lead to theft of unattended laptops
11) If assets are left unattended off premises, it could get stolen or hacked
12) If anti-virus is not updated (or patch updates not installed) regularly it could lead to malware attack / virus infection
13) If the backup process is inadequate, it may lead to loss of data
14) If Intellectual Property (IP) related requirements are not known, it is possible that the organisation may have its IP stolen or legal action for using someone else's IP.
15) If records are not stored appropriately, it may get damaged or subject to tampering
16) If staff members are unaware of Personal Information and applicable controls, it may lead to leak of sensitive data
17) If managers are unable to do a thorough review of privacy compliance, it may lead to missing of privacy and security related lapses or vulnerabilities
18) With the Cloud products becoming more widely available there will be larger & more complex products and services handled by the organisation, it may lead to the shortfall of adequately trained resources if not acted upon
19) Inadequate Business Continuity measures for the organisations
20) If infrastructural resource capacity provided is insufficient, it may lead to the system/s being unavailable or result in performance problems
21) If document is not inspected properly before Uploading documents to shared online repositories, it may lead to breach of confidential information
22) If the business does not come in as planned, then organisations may have a surplus of resources
23) Non availability of Managers / key resources in the organisations due to exit / change of employment
24) If any privacy or security requirements required by the certain geographical region are not addressed, it could lead to security violation and possible legal action

25) If the staff member exit process is weak then the asset (Laptops which contain information, or any other asset allocated to the staff member) may be lost

26) If there is no clear segregation of the different environments (development, testing, etc.), it may lead to unauthorised / unintended changes to a system

27) If software installations are not restricted it could lead to malware and hacking attacks

28) If privacy and security requirements are not propagated to contractors, vulnerability may be introduced into the applications or sensitive data may get leaked

29) If oversight of supplier activities is inadequate, then there is a possibility that security breach may occur from supplier side

30) If changes in supplier agreements or services is not fully known and managed there is a possibility of changes causing new vulnerabilities or breaches increase.

31) If the technical review for internal applications is not regular or adequate, it may lead to security breaches or vulnerabilities.

32) Lack of change management procedures can lead to unauthorised changes in the applications

33) Inadequate regression testing can lead to improper changes that can affect critical application functionality

34) If privileged access rights are not restricted and controlled, it could lead to misuse of systems

35) Lack of effective post-employment responsibilities may cause leak of sensitive information

36) If user registration process is weak it could lead to unauthorised persons gaining admission to the network and systems of the company

37) If background screening of staff members is not effective, individuals with incorrect / fake credentials may get hired

38) The lack of terms and conditions can cause staff members or contractors to intentionally or inadvertently cause a privacy or security breach

39) If all applicable laws are not identified it may be possible that some legal requirements are not met

40) If access control policy is not in place or inadequate, then it could lead to issues due to unauthorised access

41) If information access restriction is inadequate, users may have access to information not meant for them

42) If access to program source code is not restricted, it may lead to unauthorised changes to the code

43) If access to in-house developed cryptographic algorithm is not restricted, it may lead to unauthorised changes to the algorithm

44) If the access authorising process is weak, it could lead to unauthorised persons having access to the organisation's network and systems

45) If utility programs capable of overriding systems and applications is not controlled, it could lead to hacking of the systems

46) If regular spot checks are not done, it may lead to theft going undetected

47) If non-formatted equipment is reused it may provide sensitive data to unauthorised persons

48) Incorrect classification of restricted assets can lead to unauthorised access to unintended users.

49) Lack of coordination among roles can lead to sub optimal use / creations of assets

50) Absence of comprehensive privacy and security assurance for software development can lead to poor customer / user experience

51) Absence of technical standards for development for Intellectual Property (IP) development can lead to poor customer / user experience

52) Wrong selection and identification of assets can lead to inadequate return on investment

53) Sensitive information and corporate networks may get compromised when accessed remotely

54) Sensitive information and corporate networks may get compromised when using mobile devices to access remotely or on public places

55) If unmasked personal information is used for testing purposes the data could be misused

56) Failure to identify personal information / sensitive information and adequate care while handling data can lead to GDPR compliance issues

57) Disclosure of personal information inadvertently would lead to GDPR compliance issues

58) Access to third party emails and storage applications would lead to loss / leaks / theft of information

59) If the password management system is weak, it can lead to poor passwords that can be hacked

60) If staff members are not aware of non-disclosure agreements, it may lead to privacy and security breaches

4.2 APPLY THE PSEUDONYMISATION TECHNIQUES

As described in the case study design (Sections 3.5.1 and 3.5.2), the pseudonymisation technique used for the case study is through cryptographic controls. The legacy datasets are masked using encryption. For the demonstration purpose, two scenarios are presented below. The demonstration is performed on two publicly available datasets.

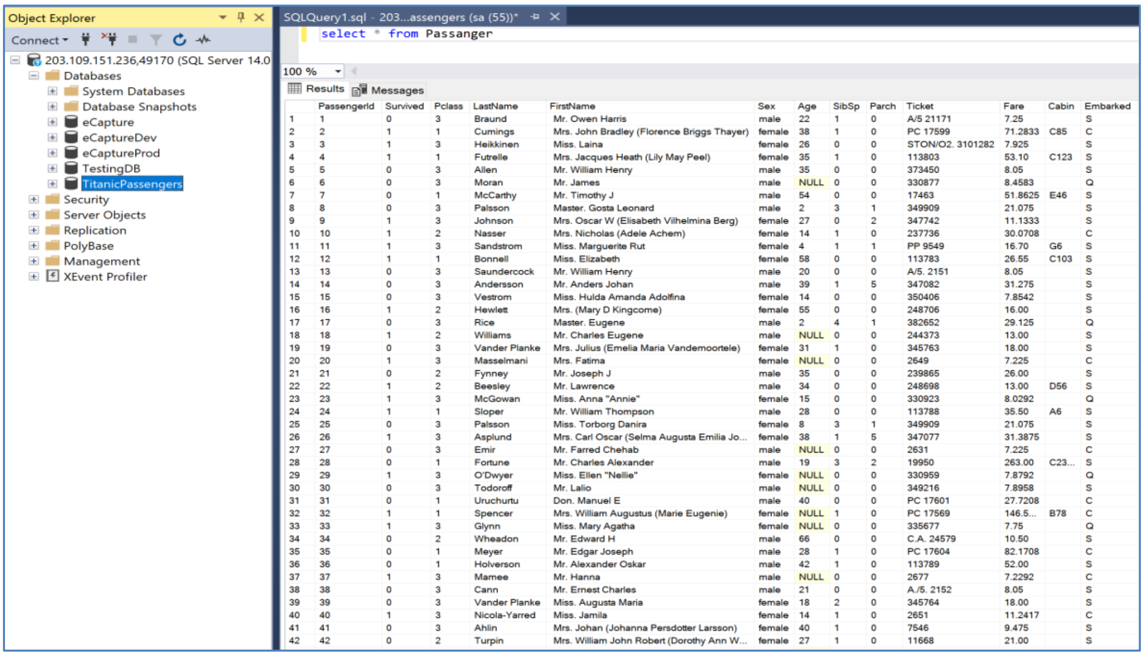
4.2.1 Database management tool for pseudonymisation

Scenario 1: Usage of Microsoft SQL Express database management tool

A publicly available dataset which had the list of Titanic passengers' details (Titanic Passengers, 2015) was used. The dataset had the details of the passengers in plain text format. The details included the personal information of the passengers such as First Name, Last Name, Sex, Age, Ticket Number, and so on.

Query 1: The dataset was imported to the Microsoft SQL Server Express 2017 database management tool and the contents were verified for the appropriateness of the data imported. The Figure 4.2.1.1 shows the snapshot from the tool.

*Select * from Passanger*



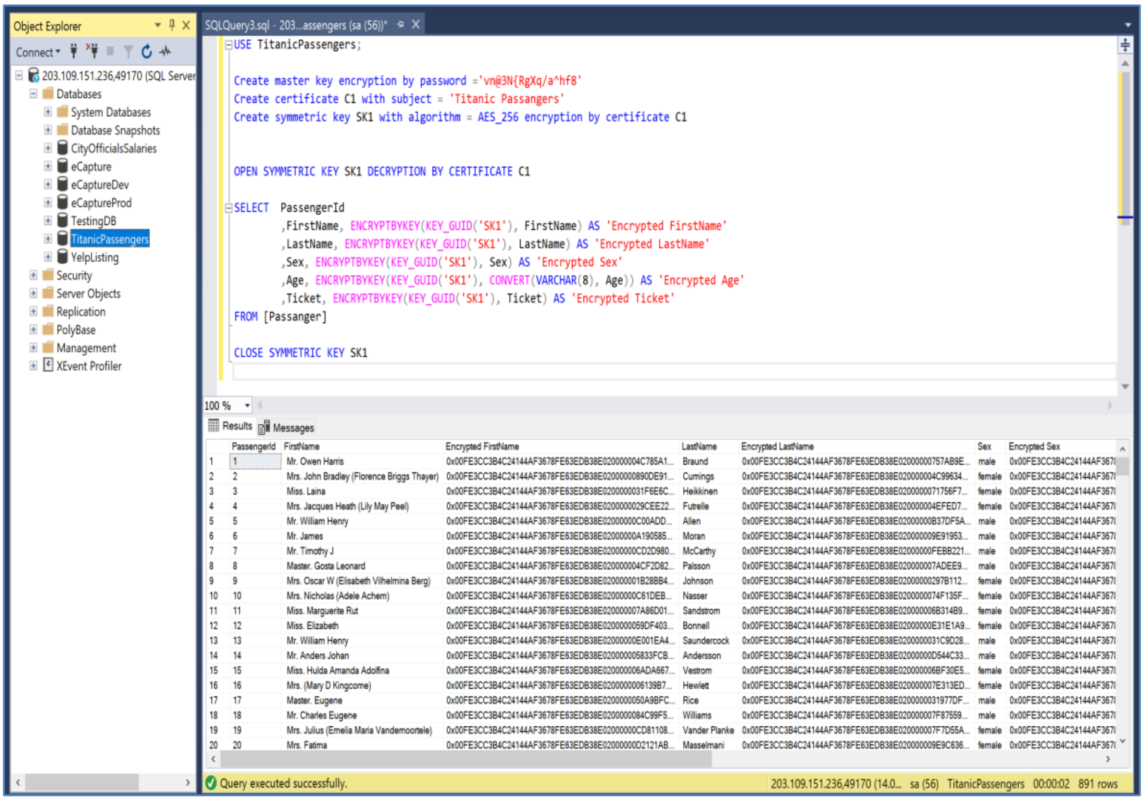
```
select * from Passanger
```

	PassengerId	Survived	Pclass	LastName	FirstName	Sex	Age	SibSp	Parch	Ticket	Fare	Cabin	Embarked
1	1	0	3	Braund	Mr. Owen Harris	male	22	1	0	A/5 21171	7.25		S
2	2	1	1	Cumings	Mrs. John Bradley (Florence Briggs Thayer)	female	38	1	0	PC 17599	71.2833	C85	C
3	3	1	3	Heikkinen	Miss. Laina	female	26	0	0	STON/O2. 3101282	7.925		S
4	4	1	1	Futrelle	Mrs. Jacques Heath (Lily May Peel)	female	35	1	0	113803	53.10	C123	S
5	5	0	3	Allen	Mr. William Henry	male	35	0	0	373450	8.05		S
6	6	0	3	Moran	Mr. James	male	NULL	0	0	330877	8.4583		Q
7	7	0	1	McCarthy	Mr. Timothy J	male	54	0	0	17463	51.8625	E46	S
8	8	0	3	Palsson	Master. Gosta Leonard	male	2	3	1	349909	21.075		S
9	9	1	3	Johnson	Mrs. Oscar W (Elisabeth Vilhelmina Berg)	female	27	0	2	347742	11.1333		S
10	10	1	2	Nasser	Mrs. Nicholas (Adele Achem)	female	14	1	0	237736	30.0708		C
11	11	1	3	Sandstrom	Miss. Marguerite Rut	female	4	1	1	PP 9549	16.70	G6	S
12	12	1	1	Bonnell	Miss. Elizabeth	female	58	0	0	113783	26.55	C103	S
13	13	0	3	Saundercock	Mr. William Henry	male	20	0	0	A/5. 2151	8.05		S
14	14	0	3	Andersson	Mr. Anders Johan	male	39	1	5	347082	31.275		S
15	15	0	3	Vestrom	Miss. Hulda Amanda Adolfina	female	14	0	0	350406	7.8542		S
16	16	1	2	Hewlett	Mrs. (Mary D Kingcome)	female	55	0	0	248706	16.00		S
17	17	0	3	Rice	Master. Eugene	male	2	4	1	382652	29.125		Q
18	18	1	2	Williams	Mr. Charles Eugene	male	NULL	0	0	244373	13.00		S
19	19	0	3	Vander Planke	Mrs. Julius (Emelia Maria Vandemoortele)	female	31	1	0	345763	18.00		S
20	20	1	3	Masselmani	Mrs. Fatima	female	NULL	0	0	2649	7.225		C
21	21	0	2	Fynney	Mr. Joseph J	male	35	0	0	239865	26.00		S
22	22	1	2	Beesley	Mr. Lawrence	male	34	0	0	248698	13.00	D56	S
23	23	1	3	McGowan	Miss. Anna "Annie"	female	15	0	0	330923	8.0292		Q
24	24	1	1	Sloper	Mr. William Thompson	male	28	0	0	113788	35.50	A6	S
25	25	0	3	Palsson	Miss. Torborg Danira	female	8	3	1	349909	21.075		S
26	26	1	3	Asplund	Mrs. Carl Oscar (Selma Augusta Emilia Jo...	female	38	1	5	347077	31.3875		S
27	27	0	3	Emir	Mr. Farred Chehab	male	NULL	0	0	2631	7.225		C
28	28	0	1	Fortune	Mr. Charles Alexander	male	19	3	2	19950	263.00	C23...	S
29	29	1	3	O'Dwyer	Miss. Ellen "Nellie"	female	NULL	0	0	330959	7.8792		Q
30	30	0	3	Todoroff	Mr. Lalio	male	NULL	0	0	349216	7.8958		S
31	31	0	1	Uruchurtu	Don. Manuel E	male	40	0	0	PC 17601	27.7208		C
32	32	1	1	Spencer	Mrs. William Augustus (Marie Eugenie)	female	NULL	1	0	PC 17569	146.5...	B78	C
33	33	1	3	Glynn	Miss. Mary Agatha	female	NULL	0	0	335677	7.75		Q
34	34	0	2	Wheadon	Mr. Edward H	male	66	0	0	C.A. 24579	10.50		S
35	35	0	1	Meyer	Mr. Edgar Joseph	male	28	1	0	PC 17604	82.1708		C
36	36	0	1	Holverson	Mr. Alexander Oskar	male	42	1	0	113789	52.00		S
37	37	1	3	Mamee	Mr. Hanna	male	NULL	0	0	2677	7.2292		C
38	38	0	3	Cann	Mr. Ernest Charles	male	21	0	0	A./5. 2152	8.05		S
39	39	0	3	Vander Planke	Miss. Augusta Maria	female	18	2	0	345764	18.00		S
40	40	1	3	Nicola-Yarred	Miss. Jamila	female	14	1	0	2651	11.2417		C
41	41	0	3	Ahlin	Mrs. Johan (Johanna Persdotter Larsson)	female	40	1	0	7546	9.475		S
42	42	0	2	Turpin	Mrs. William John Robert (Dorothy Ann W...	female	27	1	0	11668	21.00		S

Figure 4.2.1.1: Values imported to the DB tool

Query 2: From the imported dataset, FirstName, LastName, Sex and Age values were encrypted using the built-in syntax. Below is the algorithm and Figure 4.2.1.2 shows the snapshot from the tool.

```
USE TitanicPassengers;
Create master key encryption by password ='vn@3N{RgXq/a^hf8'
Create certificate C1 with subject = 'Titanic Passangers'
Create symmetric key SK1 with algorithm = AES_256 encryption by certificate C1
OPEN SYMMETRIC KEY SK1 DECRYPTION BY CERTIFICATE C1
SELECT PassengerId
        ,FirstName, ENCRYPTBYKEY(KEY_GUID('SK1'), FirstName) AS
'Encrypted FirstName'
        ,LastName, ENCRYPTBYKEY(KEY_GUID('SK1'), LastName) AS
'Encrypted LastName'
        ,Sex, ENCRYPTBYKEY(KEY_GUID('SK1'), Sex) AS
'Encrypted Sex'
        ,Age,ENCRYPTBYKEY(KEY_GUID('SK1'),
CONVERT(VARCHAR(8), Age)) AS 'Encrypted Age'
        ,Ticket, ENCRYPTBYKEY(KEY_GUID('SK1'), Ticket) AS 'Encrypted
Ticket'
FROM [Passanger]
CLOSE SYMMETRIC KEY SK1
```



```
USE TitanicPassengers;

Create master key encryption by password ='vn@3N{RgXq/a^hf8'
Create certificate C1 with subject = 'Titanic Passangers'
Create symmetric key SK1 with algorithm = AES_256 encryption by certificate C1


OPEN SYMMETRIC KEY SK1 DECRYPTION BY CERTIFICATE C1

SELECT  PassengerId
        ,FirstName, ENCRYPTBYKEY(KEY_GUID('SK1'), FirstName) AS 'Encrypted FirstName'
        ,LastName, ENCRYPTBYKEY(KEY_GUID('SK1'), LastName) AS 'Encrypted LastName'
        ,Sex, ENCRYPTBYKEY(KEY_GUID('SK1'), Sex) AS 'Encrypted Sex'
        ,Age, ENCRYPTBYKEY(KEY_GUID('SK1'), CONVERT(VARCHAR(8), Age)) AS 'Encrypted Age'
        ,Ticket, ENCRYPTBYKEY(KEY_GUID('SK1'), Ticket) AS 'Encrypted Ticket'
FROM [Passanger]

CLOSE SYMMETRIC KEY SK1
```

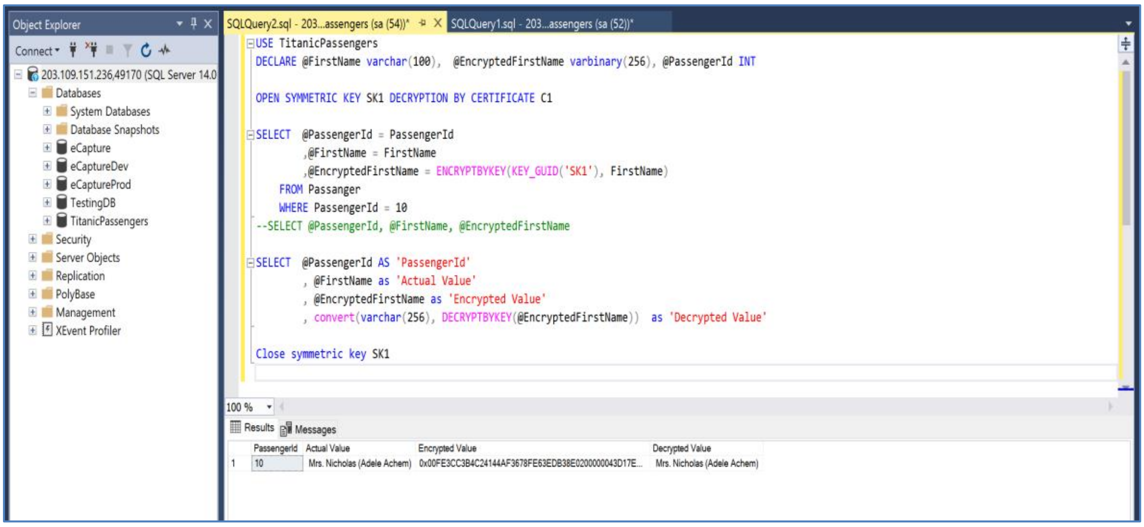
	PassengerId	FirstName	Encrypted FirstName	LastName	Encrypted LastName	Sex	Encrypted Sex
1	1	Mr. Owen Harris	0x00FE3CC3B4C24144AF3678FE63EDB38E020000004C785A1...	Braund	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000757AB9E...	male	0x00FE3CC3B4C24144AF367
2	2	Mrs. John Bradley (Florence Briggs Thayer)	0x00FE3CC3B4C24144AF3678FE63EDB38E020000000890DE91...	Cumings	0x00FE3CC3B4C24144AF3678FE63EDB38E020000004C99634...	female	0x00FE3CC3B4C24144AF367
3	3	Miss. Laina	0x00FE3CC3B4C24144AF3678FE63EDB38E0200000031F6E6C...	Heikkinen	0x00FE3CC3B4C24144AF3678FE63EDB38E020000071756F7...	female	0x00FE3CC3B4C24144AF367
4	4	Mrs. Jacques Heath (Lily May Peel)	0x00FE3CC3B4C24144AF3678FE63EDB38E020000029CEE22...	Futrelle	0x00FE3CC3B4C24144AF3678FE63EDB38E020000004EFED7...	female	0x00FE3CC3B4C24144AF367
5	5	Mr. William Henry	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000C00ADD...	Allen	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000B37DF5A...	male	0x00FE3CC3B4C24144AF367
6	6	Mr. James	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000A190585...	Moran	0x00FE3CC3B4C24144AF3678FE63EDB38E020000009E91953...	male	0x00FE3CC3B4C24144AF367
7	7	Mr. Timothy J	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000CD2D980...	McCarthy	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000FEBB221...	male	0x00FE3CC3B4C24144AF367
8	8	Master. Gosta Leonard	0x00FE3CC3B4C24144AF3678FE63EDB38E020000004CF2D82...	Palsson	0x00FE3CC3B4C24144AF3678FE63EDB38E020000007ADEE9...	male	0x00FE3CC3B4C24144AF367
9	9	Mrs. Oscar W (Elisabeth Vilhelmina Berg)	0x00FE3CC3B4C24144AF3678FE63EDB38E020000001B28BB4...	Johnson	0x00FE3CC3B4C24144AF3678FE63EDB38E0200000297B112...	female	0x00FE3CC3B4C24144AF367
10	10	Mrs. Nicholas (Adele Achem)	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000C61DEB...	Nasser	0x00FE3CC3B4C24144AF3678FE63EDB38E020000074F135F...	female	0x00FE3CC3B4C24144AF367
11	11	Miss. Marguerite Rut	0x00FE3CC3B4C24144AF3678FE63EDB38E020000007A86D01...	Sandstrom	0x00FE3CC3B4C24144AF3678FE63EDB38E020000006B314B9...	female	0x00FE3CC3B4C24144AF367
12	12	Miss. Elizabeth	0x00FE3CC3B4C24144AF3678FE63EDB38E020000059DF403...	Bonnell	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000E31E1A9...	female	0x00FE3CC3B4C24144AF367
13	13	Mr. William Henry	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000E001EA4...	Saundercock	0x00FE3CC3B4C24144AF3678FE63EDB38E020000031C9D28...	male	0x00FE3CC3B4C24144AF367
14	14	Mr. Anders Johan	0x00FE3CC3B4C24144AF3678FE63EDB38E020000005833FCB...	Andersson	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000D544C33...	male	0x00FE3CC3B4C24144AF367
15	15	Miss. Hulda Amanda Adolfina	0x00FE3CC3B4C24144AF3678FE63EDB38E020000006ADA667...	Vestrom	0x00FE3CC3B4C24144AF3678FE63EDB38E020000006BF30E5...	female	0x00FE3CC3B4C24144AF367
16	16	Mrs. (Mary D Kingcome)	0x00FE3CC3B4C24144AF3678FE63EDB38E0200000006139B7...	Hewlett	0x00FE3CC3B4C24144AF3678FE63EDB38E020000007E313ED...	female	0x00FE3CC3B4C24144AF367
17	17	Master. Eugene	0x00FE3CC3B4C24144AF3678FE63EDB38E0200000050A9BFC...	Rice	0x00FE3CC3B4C24144AF3678FE63EDB38E020000031977DF...	male	0x00FE3CC3B4C24144AF367
18	18	Mr. Charles Eugene	0x00FE3CC3B4C24144AF3678FE63EDB38E020000084C99F5...	Williams	0x00FE3CC3B4C24144AF3678FE63EDB38E020000007F87559...	male	0x00FE3CC3B4C24144AF367
19	19	Mrs. Julius (Emelia Maria Vandemoortele)	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000CD81108...	Vander Planke	0x00FE3CC3B4C24144AF3678FE63EDB38E020000007F7D55A...	female	0x00FE3CC3B4C24144AF367
20	20	Mrs. Fatima	0x00FE3CC3B4C24144AF3678FE63EDB38E02000000D2121AB...	Masselmani	0x00FE3CC3B4C24144AF3678FE63EDB38E020000009E9C636...	female	0x00FE3CC3B4C24144AF367

Query executed successfully.   203.109.151.236,49170 (14.0...   sa (56)   TitanicPassengers   00:00:02   891 rows

Figure 4.2.1.2: Values encrypted in the DB tool

Query 3: To ensure that the encrypted value was not corrupted, a random value was decrypted to check the integrity. Below is the algorithm, and the Figure 4.2.1.3 depicts the snapshot from the tool.

```
USE TitanicPassengers
DECLARE @FirstName varchar(100), @EncryptedFirstName varbinary(256),
@PassengerId INT
OPEN SYMMETRIC KEY SK1 DECRYPTION BY CERTIFICATE C1
SELECT @PassengerId = PassengerId
        ,@FirstName = FirstName
        ,@EncryptedFirstName = ENCRYPTBYKEY(KEY_GUID('SK1'),
FirstName)
      FROM Passanger
      WHERE PassengerId = 10
SELECT @PassengerId AS 'PassengerId'
        , @FirstName as 'Actual Value'
        , @EncryptedFirstName as 'Encrypted Value'
        ,convert(varchar(256), DECRYPTBYKEY(@EncryptedFirstName)) as
'Decrypted Value'
CLOSE SYMMETRIC KEY SK1
```



```
USE TitanicPassengers
DECLARE @FirstName varchar(100),  @EncryptedFirstName varbinary(256), @PassengerId INT

OPEN SYMMETRIC KEY SK1 DECRYPTION BY CERTIFICATE C1

SELECT  @PassengerId = PassengerId
       ,@FirstName = FirstName
       ,@EncryptedFirstName = ENCRYPTBYKEY(KEY_GUID('SK1'), FirstName)
    FROM Passanger
    WHERE PassengerId = 10
--SELECT @PassengerId, @FirstName, @EncryptedFirstName

SELECT  @PassengerId AS 'PassengerId'
        , @FirstName as 'Actual Value'
        , @EncryptedFirstName as 'Encrypted Value'
        , convert(varchar(256), DECRYPTBYKEY(@EncryptedFirstName))  as 'Decrypted Value'

Close symmetric key SK1
```

	PassengerId	Actual Value	Encrypted Value	Decrypted Value
1	10	Mrs. Nicholas (Adele Achem)	0x00FE3CC3B4C24144AF3678FE63EDB38E0200000043D17E...	Mrs. Nicholas (Adele Achem)

Figure 4.2.1.3: Values decrypted in the DB tool

4.2.2 A utility tool for pseudonymisation

The tool is GUI based and can be used in conjunction with the data sets or used as stand-alone for masking the table values. If entities are using simple MS excel documents with personal information in them, they may utilise this tool to generate the pseudonym and mask the data.

Scenario 2: Development of a GUI based software utility tool to mask the values in an excel document

A publicly available dataset which had the list of City Official's salaries for the City of Phoenix, Arizona (City Official's salaries for the City of Phoenix, Arizona, 2015) was used. The dataset had the details of the officials in plain text format. The details included the personal information of the passengers such as First Name, Last Name, Designation and Salary.

Snapshot of the GUI based tool (No values entered)

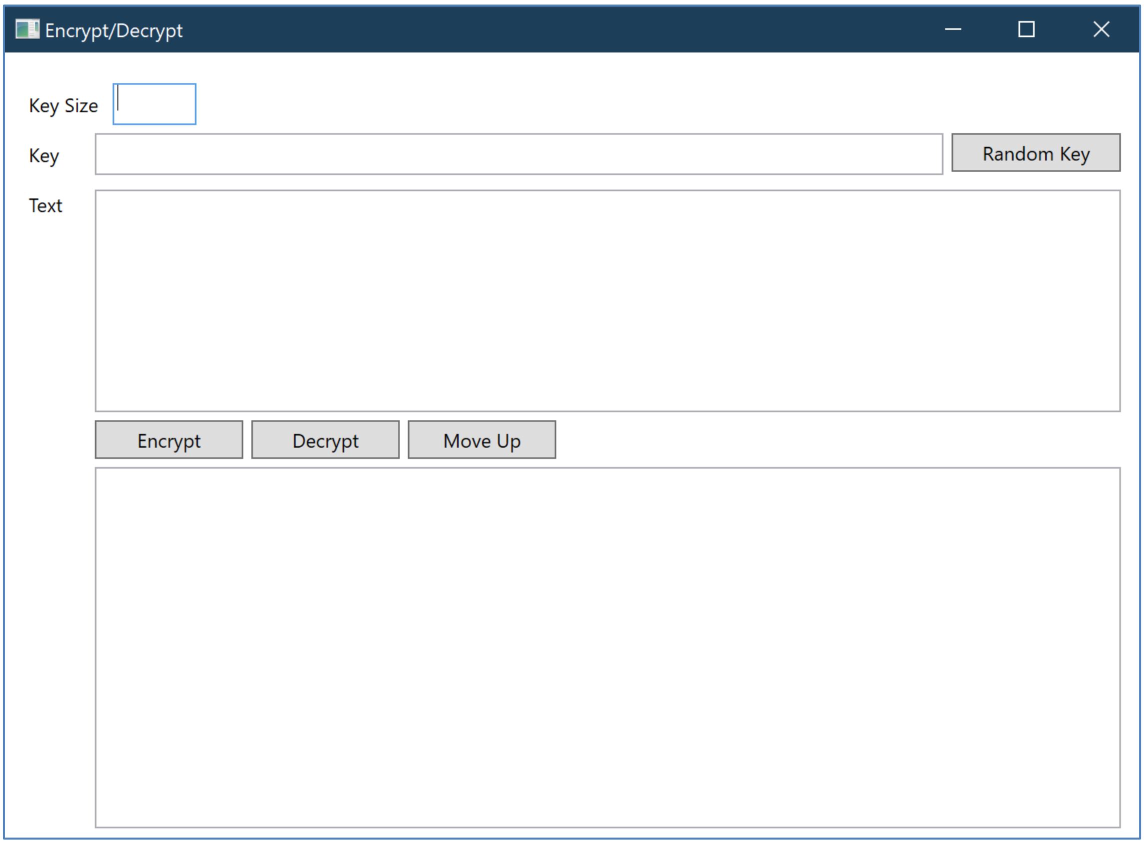


Figure 4.2.2.1: No values entered in the tool

To mask the values, the key length was chosen as *20*. (The key size can be determined as per the user’s choice)

For each of the column, different keys were generated as listed below:

Last Name: QU1+A^BbM*}MU!tOLA&e

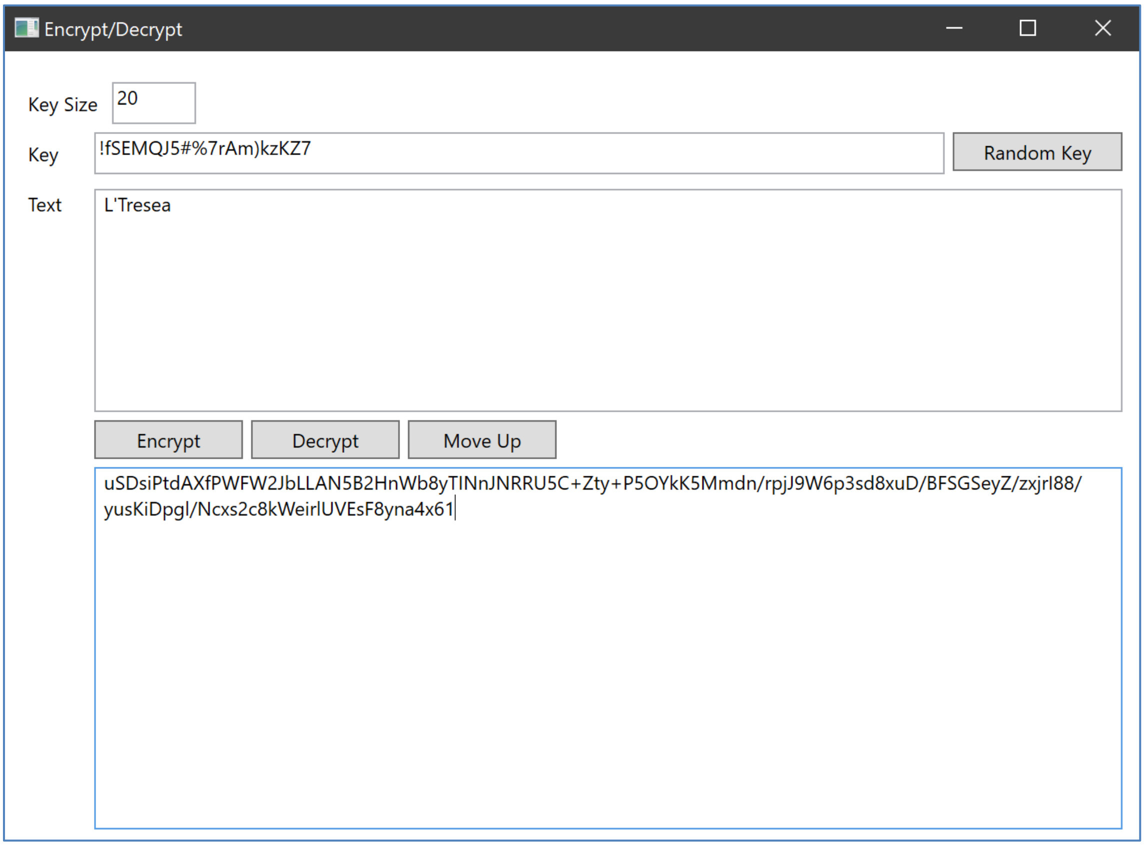
First Name: !fSEMQJ5#%7rAm)kzKZ7

Designation: OW(Q=m6xk5A-!$9%(e9x

Salary: I^Au5_9h}8SDqyO3hEp0

The length of the encrypted value is 128 bits.

A sample Snapshot of the GUI based tool (Values entered - encrypt)



Key Size 20

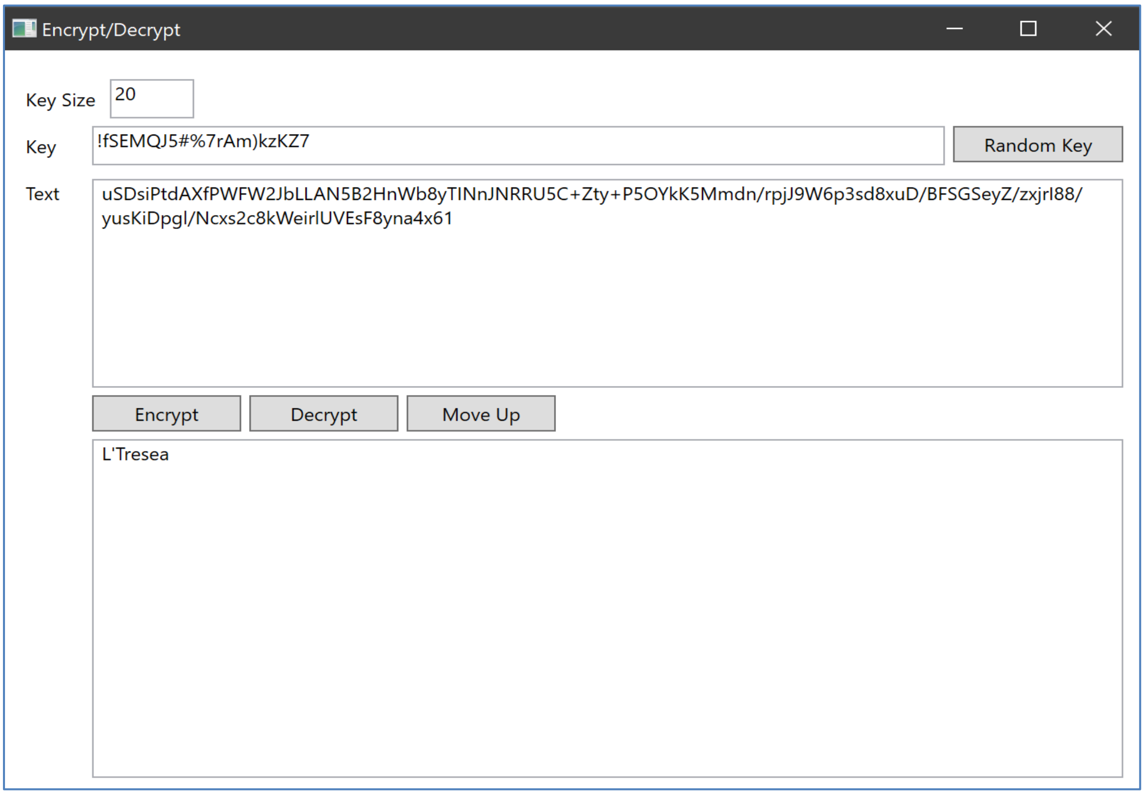
Key !fSEMQJ5#%7rAm)kzKZ7

Text L'Tresea

uSDsiPtdAXfPWFW2JbLLAN5B2HnWb8yTINnJNRRU5C+Zty+P5OYkK5Mmdn/rpjJ9W6p3sd8xuD/BFSGSeyZ/zxjrl88/
yusKiDpgl/Ncxs2c8kWeirlUVEsF8yna4x61

Figure 4.2.2.2: Values entered, and text is encrypted

Snapshot of the GUI based tool (Values entered - decrypt)



Key Size 20

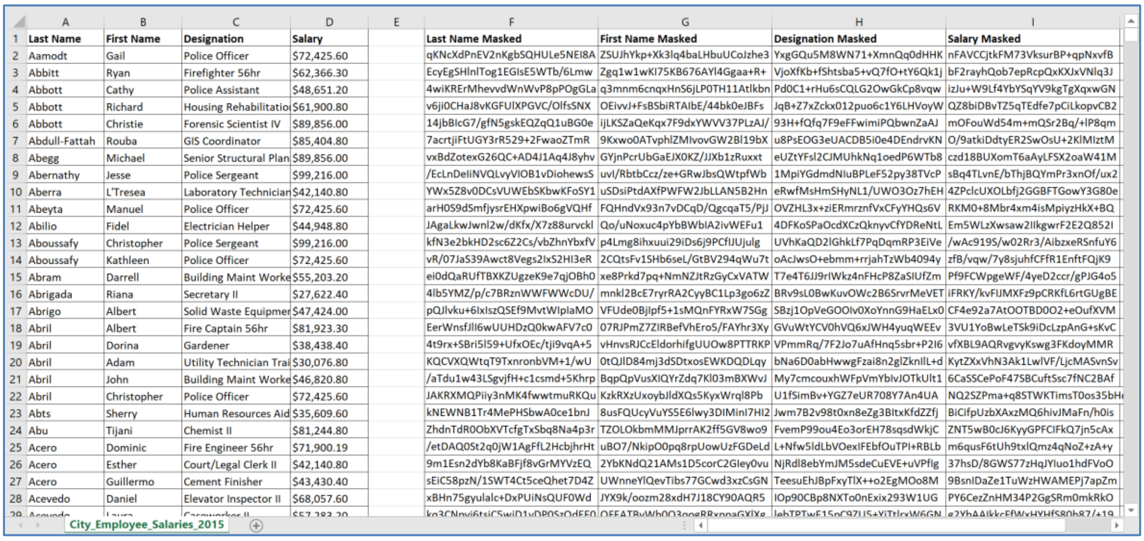
Key !fSEMQJ5#%7rAm)kzKZ7

Text uSDsiPtdAXfPWFW2JbLLAN5B2HnWb8yTINnJNRRU5C+Zty+P5OYkK5Mmdn/rpjJ9W6p3sd8xuD/BFSGSeyZ/zxjrl88/
yusKiDpgl/Ncxs2c8kWeirlUVEsF8yna4x61

L'Tresea

Figure 4.2.2.3: Values entered, and text is decrypted

Snapshot of the excel document with and without the masked values.



	A	B	C	D	E	F	G	H	I
1	**Last Name**	**First Name**	**Designation**	**Salary**		**Last Name Masked**	**First Name Masked**	**Designation Masked**	**Salary Masked**
2	Aamodt	Gail	Police Officer	$72,425.60		qKNcXdPnEV2nKgbSQHULe5NEI8A	ZSUJhYkp+Xk3lq4baLHbuUCoJzhe3	YxgGQu5M8WN71+XmnQq0dHHK	nFAVCCjtkFM73VksurBP+qpNxvfB
3	Abbitt	Ryan	Firefighter 56hr	$62,366.30		EcyEgSHlnlTog1EGIsE5WTb/6Lmw	Zgq1w1wKI75KB676AYl4Ggaa+R+	VjoXfKb+fShtsba5+vQ7fO+tY6Qk1j	bF2rayhQob7epRcpQxKXJxVNlq3J
4	Abbott	Cathy	Police Assistant	$48,651.20		4wiKRErMhevvdWnWvP8pPOgGLa	q3mnm6cnqxHnS6jLP0TH11Atlkbn	Pd0C1+rHu6sCQLG2OwGkCp8vqw	izJu+W9Lf4YbYSqYV9kgTgXqxwGN
5	Abbott	Richard	Housing Rehabilitatio	$61,900.80		v6ji0CHaJ8vKGFUlXPGVC/OlfsSNX	OEivvJ+FsBSbiRTAIbE/44bk0eJBFs	JqB+Z7xZckx012puo6c1Y6LHVoyW	QZ8biDBvTZ5qTEdfe7pCiLkopvCB2
6	Abbott	Christie	Forensic Scientist IV	$89,856.00		14jbBIcG7/gfN5gskEQZqQ1uBG0e	ijLKSZaQeKqx7F9dxYWVV37PLzAJ/	93H+fQfq7F9eFFwimiPQbwnZaAJ	mOFouWd54m+mQSr2Bq/+lP8qm
7	Abdull-Fattah	Rouba	GIS Coordinator	$85,404.80		7acrtjiFtUGY3rR529+2FwaoZTmR	9Kxwo0ATvphlZMIvovGW2Bl19bX	u8PsEOG3eUACDB5i0e4DEndrvKN	O/9atkiDdtyER2SwOsU+2KlMIztM
8	Abegg	Michael	Senior Structural Plan	$89,856.00		vxBdZotexG26QC+AD4J1Aq4J8yhv	GYjnPcrUbGaEJX0KZ/JJXb1zRuxxt	eUZtYFsl2CJMUhkNq1oedP6WTb8	czd18BUXomT6aAyLFSX2oaW41M
9	Abernathy	Jesse	Police Sergeant	$99,216.00		/EcLnDeliNVQLvyVIOB1vDiohewsS	uvI/RbtbCcz/ze+GRwJbsQWtpfWb	1MpiYGdmdNIuBPLeF52py38TVcP	sBq4TLvnE/bThjBQYmPr3xnOf/ux2
10	Aberra	L'Tresea	Laboratory Technician	$42,140.80		YWx5Z8v0DCsVUWEbSKbwKFoSY1	uSDsiPtdAXfPWFW2JbLLAN5B2Hn	eRwfMsHmSHyNL1/UWO3Oz7hEH	4ZPclcUXOLbfj2GGBFTGowY3G80e
11	Abeyta	Manuel	Police Officer	$72,425.60		arH0S9dSmfjysrEHXpwiBo6gVQHf	FQHndVx93n7vDCqD/QgcqaT5/PjJ	OVZHL3x+ziERmrznfVxCFyYHQs6V	RKM0+8Mbr4xm4isMpiyzHkX+BQ
12	Abilio	Fidel	Electrician Helper	$44,948.80		JAgaLkwJwnl2w/dKfx/X7z88urvckl	Qo/uNoxuc4pYbBWbIA2ivWEFu1	4DFKoSPaOcdXCzQknyvCfYDReNtL	Em5WLzXwsaw2IlkgwrF2E2Q852I
13	Aboussafy	Christopher	Police Sergeant	$99,216.00		kfN3e2bkHD2sc6Z2Cs/vbZhnYbxfV	p4Lmg8ihxuui29iDs6j9PCfIJUjulg	UVhKaQD2lGhkLf7PqDqmRP3EiVe	/wAc919S/w02Rr3/AibzxeRSnfuY6
14	Aboussafy	Kathleen	Police Officer	$72,425.60		vR/07JaS39Awct8Vegs2IxS2HI3eR	2CQtsFv1SHb6seL/GtBV294qWu7t	oAcJwsO+ebmm+rrjahTzWb4094y	zfB/vqw/7y8sjuhfCFfR1EnftFQjK9
15	Abram	Darrell	Building Maint Worke	$55,203.20		ei0dQaRUfTBXKZUgzeK9e7qjOBh0	xe8Prkd7pq+NmNZJtRzGyCxVATW	T7e4T6JJ9rIWkz4nFHcP8ZaSIUfZm	Pf9FCWpgeWF/4yeD2ccr/gPJG4o5
16	Abrigada	Riana	Secretary II	$27,622.40		4lb5YMZ/p/c7BRznWWFWWcDU/	mnkl2BcE7ryrRA2CyyBC1Lp3go6zZ	BRv9sL0BwKuvOWc2B6SrvrMeVET	iFRKY/kvFIJMXFz9pCRKfL6rtGUgBE
17	Abrigo	Albert	Solid Waste Equipmer	$47,424.00		pQJlvku+6IxIszQSEf9MvtWIplaMO	VFUde0BjIpf5+1sMQnFYRxW7SGg	SBzj1OpVeGOOIv0XoYnnG9HaELx0	CF4e92a7AtOOTBD0O2+eOufXVM
18	Abril	Albert	Fire Captain 56hr	$81,923.30		EerWnsfJll6wUUHDzQ0kwAFV7c0	07RJPmZ7ZIRBefVhEro5/FAYhr3Xy	GVuWtYCV0hVQ6xJWH4yuqWEEv	3VU1YoBwLeTSk9iDcLzpAnG+sKvC
19	Abril	Dorina	Gardener	$38,438.40		4t9rx+SBri5l59+UfxOEc/tji9vqA+5	vHnvsRJCcEldorhifgUUOw8PTTRKP	VPmmRq/7F2Jo7uAfHnq5sbr+P2I6	vfXBL9AQRvgvyKswg3FKdoyMMR
20	Abril	Adam	Utility Technician Trai	$30,076.80		KQCVXQWtqT9TxnronbVM+1/wU	0tQJlD84mj3dSDtxosEWKDQDLqy	bNa6D0abHwwgFzai8n2glZknIlL+d	KytZXxVhN3Ak1LwlVF/LjcMASvnSv
21	Abril	John	Building Maint Worke	$46,820.80		/aTdu1w43LSgvjfH+c1csmd+5Khrp	BqpQpVusXIQYrZdq7Kl03mBXWvJ	My7cmcouxhWFpVmYbIvJOTkUlt1	6CaSSCePoF47SBCuftSsc7fNC2BAf
22	Abril	Christopher	Police Officer	$72,425.60		JAKRXMQPiiy3nMK4fwwtmuRKQu	KzkRXzUxoybJldXQs5KyxWrql8Pb	U1fSimBv+YGZ7eUR708Y7An4UA	NQ2SZPma+q8STWKTimsT0os35bH
23	Abts	Sherry	Human Resources Aid	$35,609.60		kNEWNB1Tr4MePHSbwA0ce1bnJ	8usFQUcyVuYS5E6lwy3DIMinI7HI2	Jwm7B2v98t0xn8eZg3BltxKfdZZfj	BiCifpUzbXAxzMQ6hivJMaFn/h0is
24	Abu	Tijani	Chemist II	$81,244.80		ZhdnTdR0ObXVTcfgTxSbq8Na4p3r	TZOLOkbmMMJprrAK2ff5GV8wo9	FvemP99ou4Eo3orEH78sqsdWkjC	ZNT5wB0cJ6KyyGPFClFkQ7jn5cAx
25	Acero	Dominic	Fire Engineer 56hr	$71,900.19		/etDAQ0St2q0jW1AgFfL2HcbjhrHt	uBO7/NkipO0pq8rpUowUzFGDeLd	L+Nfw5ldLbVOexIFEbfOuTPI+RBLb	m6qusF6tUh9txlQmz4qNoZ+zA+y
26	Acero	Esther	Court/Legal Clerk II	$42,140.80		9m1Esn2dYb8KaBFjf8vGrMYVzEQ	2YbKNdQ21AMs1D5corC2Gley0vu	NjRdl8ebYmJM5sdeCuEVE+uVPflg	37hsD/8GWS77zHqJYIuo1hdFVoO
27	Acero	Guillermo	Cement Finisher	$43,430.40		sEiC58pzN/1SWT4Ct5ceQhet7D4Z	UWnneYlQevTibs77GCwd3xzCsGN	TeesuEhJBpFxyTlX++o2EgMOo8M	9BsnIDaZe1TuWzHWAMEPj7apZm
28	Acevedo	Daniel	Elevator Inspector II	$68,057.60		xBHn75gyulalc+DxPUiNsQUF0Wd	JYX9k/oozm28xdH7J18CY90AQR5	IOp90CBp8NXTo0nExix293W1UG	PY6CezZnHM34P2GgSRm0mkRkO
29	Acevedo	Laura	Caseworker II	$57,283.20		kq3CNpvi6tsiC5wiD1vDP0SzQdEF0	OFFATBvWh0O3qogRRxnnaGXlXg	lehTPTwF15nC9ZU5+YiTtlrxW6GN	g2YbAAlkkcFfWxHYHfS80h87/+19

Figure 4.2.2.4: All the values encrypted in an MS excel document

The necessary level of security must be defined based on a risk assessment, considering the form, resistance and performance of the recommended cryptographic algorithm. Such an evaluation could be used to decide if data encryption control is necessary, what sort of control must be implemented and what objective and management procedures must be implemented. Determining if a data encryption option is suitable must be considered as part of the broader risk management and control application process.

4.3 GUI BASED PSEUDONYMISATION TOOL

Below is the algorithm used to develop the GUI based pseudonymisation tool. The algorithm could be reused with suitable programming language modifications and implemented for generic usage. The algorithms are split into two components, one being the encryption-decryption engine and the other being the key generator. These algorithms formed the basis for demonstrating pseudonymisation in the section 4.2.2. The code was implemented using the .NET framework on a Windows machine.

4.3.1 Source code for encryption and decryption

The implementation was done based on Protecting The CDN Application Files From Unauthorised Requests (Ghanbari, 2015) and Getting started with Steganography (hide information) on Images with C# (Delgado, 2017) to develop the solution. The following criteria were followed to arrive at the algorithm:

To encrypt:

In the encryption algorithm, to evaluate the size of the key in bits, a constant is used. The max key size considered was 256. To arrive at the uniform number of bytes, the key size was divided by 8 within the code described. The constant defines the amount of loops for the function to generate the password bytes. Salt and IV (Initialisation Vector) are produced at random every time but appended to the encrypted cipher text because the same values of Salt and IV are used while decrypting. Build the final bytes by concatenating the random bytes of salt, random bytes of IV and bytes of cipher.

To decrypt:

Get the full byte sequence comprising of the 32 Salt bytes, the 32 IV bytes and the 64 Cyphertext bytes. Obtain the bytes of salt from the available bytes of Cyphertext by removing the first 32 bytes. Obtain the bytes of IV from the available bytes of Cyphertext by retrieving the next 32 bytes. Obtain the actual bytes of cipher text by deleting the first 64 bytes from the string of Cyphertext.

```
using System;
using System.Configuration;
using System.IO;
using System.Linq;
using System.Security.Cryptography;
using System.Text;
namespace DataEncrypterDecrypter
{
    public class CryptoEngine3
    {
        private const int Keysize = 256;
        private const int DerivationIterations = 1000;
        public static string Encrypt(string plainText, string passPhrase)
        {
            var saltStringBytes = Generate256BitsOfRandomEntropy();
            var ivStringBytes = Generate256BitsOfRandomEntropy();
            var plainTextBytes = Encoding.UTF8.GetBytes(plainText);
            using (var password = new Rfc2898DeriveBytes(passPhrase,
saltStringBytes, DerivationIterations))
            {
                var keyBytes = password.GetBytes(Keysize / 8);
                using (var symmetricKey = new RijndaelManaged())
                {
                    symmetricKey.BlockSize = 256;
                    symmetricKey.Mode = CipherMode.CBC;
```

```
          symmetricKey.Padding = PaddingMode.PKCS7;
          using (var encryptor = symmetricKey.CreateEncryptor(keyBytes,
ivStringBytes))
          {
            using (var memoryStream = new MemoryStream())
            {
              using (var cryptoStream = new CryptoStream(memoryStream,
encryptor, CryptoStreamMode.Write))
              {
                cryptoStream.Write(plainTextBytes, 0,
plainTextBytes.Length);
                cryptoStream.FlushFinalBlock();
                var cipherTextBytes = saltStringBytes;
                cipherTextBytes =
cipherTextBytes.Concat(ivStringBytes).ToArray();
                cipherTextBytes =
cipherTextBytes.Concat(memoryStream.ToArray()).ToArray();
                memoryStream.Close();
                cryptoStream.Close();
                return Convert.ToBase64String(cipherTextBytes);
              }
            }
          }
        }
      }
    }

    public static string Decrypt(string cipherText, string passPhrase)
    {
      var cipherTextBytesWithSaltAndIv =
Convert.FromBase64String(cipherText);
      var saltStringBytes = cipherTextBytesWithSaltAndIv.Take(Keysize /
8).ToArray();
      var ivStringBytes = cipherTextBytesWithSaltAndIv.Skip(Keysize /
8).Take(Keysize / 8).ToArray();
      var cipherTextBytes = cipherTextBytesWithSaltAndIv.Skip((Keysize / 8) *
2).Take(cipherTextBytesWithSaltAndIv.Length - ((Keysize / 8) * 2)).ToArray();
      using (var password = new Rfc2898DeriveBytes(passPhrase,
saltStringBytes, DerivationIterations))
      {
        var keyBytes = password.GetBytes(Keysize / 8);
        using (var symmetricKey = new RijndaelManaged())
        {
          symmetricKey.BlockSize = 256;
```

```
               symmetricKey.Mode = CipherMode.CBC;
               symmetricKey.Padding = PaddingMode.PKCS7;
               using (var decryptor = symmetricKey.CreateDecryptor(keyBytes,
ivStringBytes))
               {
                  using (var memoryStream = new MemoryStream(cipherTextBytes))
                  {
                     using (var cryptoStream = new CryptoStream(memoryStream,
decryptor, CryptoStreamMode.Read))
                     {
                        var plainTextBytes = new byte[cipherTextBytes.Length];
                        var decryptedByteCount = cryptoStream.Read(plainTextBytes,
0, plainTextBytes.Length);
                        memoryStream.Close();
                        cryptoStream.Close();
                        return Encoding.UTF8.GetString(plainTextBytes, 0,
decryptedByteCount);
                     }
                  }
               }
            }
         }
      }
      private static byte[] Generate256BitsOfRandomEntropy()
      {
         var randomBytes = new byte[32];
         using (var rngCsp = new RNGCryptoServiceProvider())
         {
            rngCsp.GetBytes(randomBytes);
         }
         return randomBytes;
      }
   }
}
```

4.3.2 Source code for key generation

The implementation was done based on RNGCryptoServiceProvider (2015) to develop the solution.

```
using System;
using System.Security.Cryptography;
using System.Text;
namespace UniqueKey
```

```
{
   public class KeyGenerator
   {
      internal static readonly char[] chars =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ123456789
0!@#$%^&*()_+=-[]}{".ToCharArray();
      public static string GetUniqueKey(int size)
      {
         byte[] data = new byte[4 * size];
         using (RNGCryptoServiceProvider crypto = new
RNGCryptoServiceProvider())
         {
            crypto.GetBytes(data);
         }
         StringBuilder result = new StringBuilder(size);
         for (int i = 0; i < size; i++)
         {
            var rnd = BitConverter.ToUInt32(data, i * 4);
            var idx = rnd % chars.Length;
            result.Append(chars[idx]);
         }
         return result.ToString();
      }
   }
}
```

4.4 CONCLUSION

Chapter 4 has demonstrated the usage of a management approach for Privacy Impact Assessment, and technical approaches like Privacy Enhancing Technologies for achieving Privacy by Design. By implementing risk assessment, all the possible risks faced by an organisation to maintain privacy of the data collected was identified. From the assessment outcome it contributed towards the identification and implementation of the pseudonymisation technique to ensure privacy through technical controls. The usage of database management tool such as the Microsoft SQL Server Express enable organisations to maintain a dataset in a secure manner. Other similar tools can also be explored to implement pseudonymisation. The software utility tool can be used in an independent environment, irrespective of the requirement to have a database management tool or not. Smaller organisations maintain their dataset through MS Excel, and such tools would enable them to secure their information.

Chapter 5

CASE ANALYSIS AND ADVICE

5.0 INTRODUCTION

From the case work it could be established that, by using Privacy Enhancing Techniques (PETs) we can achieve Privacy by Design. The pseudonymisation techniques adopted through the usage of Microsoft SQL Server Express tool and the software utility tool enabled the researcher to successfully mask the personal information and values in the data tables. The data which were previously not secured through pseudonymisation techniques are now masked and secured. Following are the analysis supporting the case work; which in tandem with the software intends to address the cleansing of legacy data for GDPR compliance.

5.1 IDENTIFY AND CLASSIFY THE INFORMATION ASSETS

As described in the case study design, the initiation of GDPR compliance is based on the ISO standards, such as the ISO 27001. Accordingly, it is implemented for GDPR compliance which begins with the identification and classification of information assets.

Organisations identify data to determine adequate safeguarding measures for the data resources. As facilities are restricted, prioritisation and identification of just what requires security will be essential. The return on investment to develop an encryption technology to safeguard data in the public domain may not be regarded as a reasonable commercial proposition. All data is generated uniformly, however not all data is of uniform value. Over all the data collected in an organisation, just about 10% is a significant benefit, a proprietary information or private data. The most important part of organisational data is the data that most or all staff members usually access to perform their entrusted activities. The rest of the data should be made publicly accessible via approved sources (Peltier, 2014).

A method for classifying assets or data is a risk-based decision process of an organisation considering legal / regulatory requirements. Data is an organisational resource and it is the responsibility of leadership to safeguard and cater for the adequate use of all resources. A method of classification of data will enable management to fulfil this legal obligation. Instruction and consultation are the roles of the information security specialist and that of the information systems staff. The ultimate decision is taken by the management of the organisation or, as described, by the owner of the asset / resource (Peltier, 2014).

While classifying the data, it is recommended to limit the number of categories of information classification. If no significantly distinct treatments are required for two probable classifications, then merge them. By listing more categories, the higher the chances of executives and staff being confused. Three or four classifications should ideally be adequate to satisfy the requirements of an organisation. Many organisations also make everything categorised as confidential to standardise the classification system. The issue with such an idea is that exceptional treatment of private data is required. Such a technique could involve the organisation to sacrifice restricted resources to protect assets that really do not require that amount of control. A sample categorisation of information classification could be as listed below (Peltier, 2014):

- Top Secret: Information that could have serious impacts on the significant advantage or business practices of the organisation, if revealed

  Examples: Strategic company plans such as procurement plans, encryption keys, identity authentication data such as passwords, PINS and documents or databases containing authentication data, source code, unannounced business performance, sensitive private data (e.g., social security number / national identification and health, financial or payment card information), product design documents, vulnerabilities in the unfixed product security, official investigation information or incidents related to security, and so on
- Confidential: Information that could infringe the privacy of people, decrease the significant advantage or harm the business, if revealed

  Examples: Customer or internal application specifications and standards, employee performance assessments and payroll documents, Employee private contact information, customer or other third-party agreements, development documentation, code inspection reports, approval information including corporate summaries and email approval chains, financial data, customer data supplied for Cloud, and so on
- Restricted (Internal use): Information accessible to a segment of the workforce when doing business activities

  Examples: Internal mails, training resources for employees, internal business strategies, confidential documentation or user manuals for customer delivery, organisational charts, business contact data, and so on

- Public: Information produced by the business that is publicly accessible via approved channels of the organisation

  Examples: Marketing brochures, annual reports published, business cards, press releases, and so on

Laws require organisations to retain specific types of records, generally for a fixed period. Inability to maintain those records for a specified minimum period may impose restrictions, financial penalties, or other embargoes on an organisation, or may place it in lawsuits at a severe disadvantage. Each organisation must therefore adopt a record management policy to set guidelines for keeping comprehensive records to help make sure that staff members are conscious about what records to maintain and how long; what records to discard and how to discard them. The capacity to incorporate specifications with a record management policy is part of an efficient data classification system. Information resources must be secured, preserved and then discarded in accordance with a policy and norms set. The data classification policy will assure that each asset is allocated to a proprietor, that a correct classification is allocated and that a set of norms for data handling will assist in document control. The record management policy requires the proprietor to include a detailed summary of the data record and the requisites for retaining the record. All such specifications will be a set of norms supporting the policy of records management (Peltier, 2014).

Merely giving prominence to a few information types without considering the perspective of use could be too vague for protecting the privacy of data subjects. Not only can this strategy deter positive or effective treatments of sensitive information, but it also fails to acknowledge adverse uses of information that are considered non-sensitive in distinct situations. Several research studies have shown that the circumstances under which data is revealed shapes social perspectives of data sensitivity. Demographic data such as name, personal contact details and location, for example, are generally considered to be marginally sensitive. However, once demographic data is associated with financial data like those of credit card numbers and its pin, the same demographic data is construed as extremely sensitive. The risk level affiliated with the sensitive data is a main factor in deciding that whether such a specified set of data is vulnerable or not (Fazlioglu, 2019).

When data controllers give prominence to a few kinds or types of information automatically or by default without contemplating why that information is being used, they can disregard the advantages and dangers of the same information in various contexts. The probability and intensity of data processing risks or rewards rely on how information is utilised and the processing context. Such an information processing and sensitivity inconsistency function presents a pertinent hurdle for policymakers seeking to develop legislation that can safeguard privacy and strengthen effective uses of information. It really is essential to confront an environment in which information is becoming increasingly complicated and omnipresent (Fazlioglu, 2019).

Classification of Information steers the specifications for security controls, and this enables protection of information to be at a scale proportional with its organisational value. Overprotection costs are neutralised, and caveats are reduced. Requirements are evident with a policy and methodology for order and responsibility. The most recognisable costs include the identification of the information classified, the implementation and tracking of controls and protective measures and the proper management of classified data. The information classification system will necessitate the type of record, the owner and the classification extent to be identified. The organisation would have a significantly improved information security system by merging such actions (Peltier, 2014).

As part of the case study, it could be observed that when the initial data set was imported to the tool, there was no placeholder to capture the record retention duration. Through information classification, it was identified that the personal information of the passengers such as First Name, Last Name, Sex, Age, Ticket Number, and so on could be classified as restricted information and that they required data masking to avoid the revelation of private data in the event of a data infringement. For the purpose of conforming to the regulation, an additional column was introduced to identify the date on which the record was created. Once the date is captured, it would become easier to identify the information that needs to be discarded / destroyed once the stipulated duration for retention of the information has been met. A data retention period is usually based on the laws that prescribe it or based on the agreement with the data subject who had shared the information. The data retention period enables the automated disposal of the information from the data set using database management systems. This ensures that organisations could not retain the information with them for a duration more than it was required for use. It would also benefit the organisation if there happens to be a data breach and all the data collected over the years would be disclosed. Implementing the data retention and disposal mechanism at database management level would ensure that all such inadvertent data disclosures could be avoided.

5.2 PERFORM PRIVACY IMPACT ASSESSMENT – RISK ASSESSMENT

As described in the case study design, the next important phase involved in cleansing of legacy data is the Privacy Impact Assessment or Risk Assessment. As described in the section 4.1, a possible list of risks was captured to mitigate or avoid the privacy related risk. Below are the insights on the necessity for risks to be identified at the early stage of organisational planning or goal setting.

Data sensitivity is often described as a parameter in the scale and intensity and complexity involved in the processing activities and its associated risks. For instance, a list of rules on the processing of classified medical data describes it as the data involving exceptionally high risks in the occurrence of breach. The GDPR establishes descriptions across the legislation that are also prevalent in policy debates on information security and privacy, for instance on the private information, authorisation and categorisation. The GDPR tends to make a limited differentiation amidst the controllers and processors, trying to impose on each controller a distinctive set of conditions. According to the GDPR, controllers appear to be more responsible for assessing and reducing the risks accompanied with processing of the information (Fazlioglu, 2019).

Privacy impact assessment (PIA) is a technique for evaluating the effect on the privacy of an initiative, legislation, application, business, commodity or other initiatives involving the private data processing and, in acquaintance with interested parties, implementing corrective measures needed to prevent or minimise detrimental effects. A PIA would involve interested parties from the inception in order to collect their points of view on how to prevent or mitigate any unwanted impacts on privacy. PIA is a method for recognising and assessing privacy risks, monitoring conformance with data protection regulations and considering ways of avoiding or mitigating those risks (Wright & De Hert, 2012).

There are different motivations as to why bureaucratic and commercial organisations perform a PIA. A risk assessment and management system must be primarily focused on a PIA. PIA advocates recognised numerous risks for an enterprise that processes or gathers personal data and additional rewards from conducting a PIA to recognise, prevent or reduce such risks. Risks may emerge from organisational weaknesses internally or threats from outside. As stated by the European Network and Information Security Agency (ENISA), differentiating the asset vulnerabilities, its threats and risks is helpful (Wright & De Hert, 2012).

Assets are business procedures and tasks, elements of information or software and hardware, network, staff members, and so on. The asset is also valued because the impact of a security incident determines the value of the asset. The cost of violating confidentiality, integrity and availability (CIA) in the wake of an eventuality is a very common basis for asset valuation. A vulnerability denotes an element of a framework or procedure of the asset that could be manipulated for the intentions besides it was meant, weaknesses, security flaws or application execution deficiencies that are probable to be at risk. A vulnerability must be manipulated by a threat to be regarded a risk. A threat can adversely affect or jeopardise the assets for example data, procedures and technologies and thus organisations. Threats might be of expected or man-made descent and may be unforeseen or intentional. There may be a threat from the inside or beyond the organisation (Wright & De Hert, 2012).

A PIA must consider not just the effects on privacy, but also the effects of the privacy compromise on an organisation. Effects can be direct or indirect. An organisation is at risk of having different implications if it does not take the necessary care over the private information it possesses. Several others too suffer in addition to the impacts for an organisation. People whose information has been breached could devote a great deal of time, resources and discomfort on recuperating from identity fraud or correcting the incorrect information. Few people might be at risk if their confidentiality or private information is jeopardised (Wright & De Hert, 2012).

PIA could help confirm that privacy is incorporated into modern processes, but the connection must be developed. PIA is usually carried out well after the primary design specifications have been established, an organisational framework has been established and has incurred substantial expenses. A genuine privacy by design would only be accomplished if the initiators and developers of new technologies recognise privacy as being among the factors they need to explore in addition to features, price and other considerations. PIA could make a significant contribution to privacy by design when the collective retrospective impact is lesser and when there are minimal negative impacts on privacy. Due to the consequence of privacy invasion projects have come across complications, where tasks have experienced troubles because of privacy interruption. The organisations and experts concerned would ideally become familiar with the experience gained and be more aware of the advantages of implementing privacy from the very beginning in the forthcoming activities. It would be advisable for privacy professionals to be involved far in advanced phases and in making key decisions on how to achieve organisational goals. It can decrease the requirement for PIA at final phases of undertaking a project (Waters, 2012).

As outlined by the UK Information Commissioner’s PIA Handbook, following are the reasons to perform Privacy Impact Assessment: 1) to recognise and oversee privacy risks, 2) to prevent nonessential expenses, 3) to prevent from unsatisfactory deliverables being put in to operation at subsequent phases, 4) to keep away from lack of confidence and credibility by resolving issues and problems, 5) to apprise the organisation's strategies for communication, and 6) to fulfil and surpass the statutory obligations (Wadhwa & Rodrigues, 2013).

Research was conducted and presented with a rundown of parameters for assessing the viability of PIAs dependent on PIA reports. The PIAF (which was set up based on the EU Privacy Impact Assessment Framework initiative) report utilised the mentioned parameters to gauge the viability of the reports related to PIA and, which aids, to evaluate the general PIA progression: 1) expeditious adoption of PIA, 2) verification of the person carrying out the PIA, 3) task details to be evaluated, its objective and any appropriate background details, 4) information flow mapping, 5) Inspecting adherence of the task with the appropriate law, 6) evaluation of privacy risks or its effects, 7) evaluation of risk avoidance or mitigation strategies or alternatives, 8) suggestions, 9) notifications, and 10) consulting with interested parties (Wadhwa & Rodrigues, 2013).

Classification of information by definition or category and prioritisation of information deemed sensitive is a key first phase in risk assessment, but this course of action is just the start of the process. Largely based on the rate of sensitivity of a section of information and the risks associated with it, the privacy of data subjects will not be completely protected. Hence, data controllers and regulatory agencies should always consider other determinants while evaluating the data processing risks, additionally to the information category or its level of sensitivity. There has been a need for broad interpretation of sensitive data and for legislation to increase safeguards to new types of information that can distinctively recognise or disclose sensitive data about data subjects. Lawmakers must focus on improving strongly acknowledged sensitive data and at the same time safeguard against the risks posed by detrimental data usage contexts (Fazlioglu, 2019).

There are several factors that an organisation needs to be cautious about information classification of different Information Security Risk Management (ISRM) related information assets. The following are the motives in this regard. 1) Some information should always remain classified in an ISRM system. These include prospective vulnerability details, annual budget of an organisation, etc. In the apparent lack of a certain information classification system, a rival organisation may collect this information and may indulge in misusing the information. Adequate classification of protection and methods can be applied to protect against unauthorised access to sensitive information. 2) Many organisations do have contractual agreements to safeguard information as per the requirements of customers or business associates. Several other interested parties are actively engaged in an organisation's ISRM system. Through adhering to regulatory and legal prerequisites, an organisation could reduce the possibility of hefty fines. 3) In certain nations and in few corporate sectors, it is essential to fulfil the legislative mandate. Since the ISRM system involves numerous confidential information concerning the organisation and its customer, it does become qualified for special information processing prerequisites. 4) An organisation that is persistently following an appropriate information classification strategy can take advantage of businesses that haven't seriously implemented information classification (Agrawal, 2017).

Assessment of risk includes identification of risk, analysis of risk and evaluation of risk. The information assets and their owners are recognised in the risk identification phase. In the subsequent stages there would be the detection of the threats to the recognised information assets, the prevailing and premeditated security and privacy enhancing techniques, the vulnerabilities that could be taken advantage and the recording of the eventualities with their implications on the recognised information assets. The risk analysis stage would take a qualitative or quantitative strategy to evaluate the effects and the probability of applicable events. The risks identified are given priority at the stage of assessing the risk according to the assessment of the risk parameters for incident circumstances leading to these risks. Risk treatment preferences are chosen depending on the results of the assessment of the risk, the anticipated financial obligation of adopting these alternatives and the anticipated advantages of these alternatives. Risks are managed to retain whenever the risk level meets the criteria for risk acceptance (Agrawal, 2017).

As part of the case study, it is observed that because of the asset considered for the study, there are vital personal information present in the data set. Keeping in mind the impact of a breach of such information, a detailed list of risks was identified. The risks identified covers most of the strategic parameters that could impact privacy of the individuals if a breach were to occur.

5.3 INITIATE TRAINING AND AWARENESS

As described in the Chapter 3, training and awareness about privacy and security is one of the crucial elements in achieving the compliance towards privacy regulations. The following are factors to be noted with respect to awareness and training.

An information technology platform faces many security risks. IT security's greatest challenge is human mistakes, both deliberate and inadvertent. This element of human mistakes can be caused in an organisational structure not only by staff members, but also by external users such as customers and vendors. Ransomware and spoofing / phishing are instances of human mistake-related attacks. Ransomware attacks are caused by human mistake as malicious hackers can access the system by pushing their victim to download malware to a computer on the network. Often it happens when a user clicks on a link or mistakenly downloads it. Spoofing / phishing attacks attempt to invite clicking a link to install malicious software by appearing to be a reliable individual or organisation. Organisations should therefore contemplate including all its customers in the information system in their information security awareness initiative. Educating individuals may result in a change in their conduct (Sari & Prasetio, 2018).

Information Security Awareness (ISA) portrays a requirement for individuals to be conscious of and dedicated to an organisation's information security activities. Also, it includes the individual's knowledge of the organisation's policies for data security. The whole idea reflects independent rational perceptions of data security and compliance with mandated policies for data security. ISA was recognised as an indispensable and crucial element for the achievement of information security objectives in enterprises. As ISA is impermanent, an organisation must regularly evaluate the ISA of its staff members and provide suitable improvement initiatives. Measurement of ISA also includes individual psychology such as understanding, behavior and attitude. They demonstrate how a person inherits a favorable or adverse way for a specific purpose (Wahyudiwan, Sucahyo & Gandhi, 2017).

Regrettably, the efficacy of security awareness initiatives is difficult to assess. It has already been established that, irrespective of their evaluated understanding and indicated objectives, most staff members would fail to comply with the security protocols of their organisation. Many organisations carry out post-training assessments to evaluate the training's effectiveness. In practice, these assessments only measure early receptivity, security awareness in a short-term and the self-reported inclination of the staff member to be secure always. If all these strategies are satisfactory, the organisation then works with a misguided perception of affirmation that staff members are conscious of best practices and will be secure (Gundu et al., 2019).

Most of them who provide information security training evaluate the effectiveness of the exercise by means of a post-evaluation exam. This analyses how far the information was conveyed and grasped. It is also popular for individuals to be questioned about their plan to function securely immediately after the exercise. If the impact of the training is not measured, organisations may be exposed to the following avoidable mistakes: 1) Promote an inadequate facility of awareness / training with no actual behavior enhancement, 2) Disrupt an efficient awareness / training activity centered on an inaccurate subjective evaluation, primarily due to a false notion that it does not change behavior or is very much demanding in terms of staff members' time, and 3) The organisation might also assume that almost everyone behaves securely regardless, and that no additional training is required. Information security has a restricted funding, so it is often necessary to defend the expenditure for the implementation of controls. Their predicted advantages must therefore be measurable if InfoSec assets are to be preserved or enhanced (Gundu et al., 2019).

Measurement of ISA could be carried out using specific areas of interest. The areas of interest represent disciplines of a policy for information security that are applicable to employees and most likely to fail to comply. The areas of interest could be such as locking of the computers, sharing of passwords, emails that are forwarded, attachments that are opened, software that are unauthorised being installed, websites which are shady in nature being accessed, internet being used inappropriately, time spent on social networking sites during worktime, social networking sites being used to post work related contents, individuals who report suspicious activities, security related events being reported, electronic devices being physically secured, sensitive documents being disposed, using removable devices, and so on (Wahyudiwan et al., 2017).

Awareness of information security revolves around two dimensions. The first dimension covers the magnitude to which the conduct of staff members in grasping information security is often defined in security measures, organisational security policies and procedures. The second dimension revolves around the magnitude to which staff members engage and work in line with good practices, sometimes described in strategies, provisions and guidelines on information security (Puspitaningrum et al., 2018).

Every organisation must ensure that their staff members are part of the security and privacy culture adopted to deliver high delivery standards to their customers. The management of the organisation offers human resources and premeditated course for the employment of the ISMS. Management facilitates the integration of information security procedures and controls with business processes and appropriate resources are accessible for system operation and maintenance. Initiatives and technologies to create, retain and enhance the Information Security Management System demonstrate management's dedication to Information Security. Management strengthens corporate information security policy and associated corporate practices that apply to all staff members. The corporate policy describes the policy's general objective and the values for managing information access.

The resource necessities for the establishment, execution, upkeep and constant enhancement of the ISMS will be chosen considering present and expected resource demands, current capabilities, limitations and what needs to be outsourced or acquired from outside suppliers. Organisation ensures that employed individuals have the necessary skills for the position based on education, training, certification and experience. Staff members need to read and comprehend information security policies and periodically complete compliance training and evaluation. Managers must receive all the client security criteria and policies stipulated in the business agreement to which members of staff are supposed to adhere. Internal assessments of skills, certifications and internal certification must be scheduled and carried out. The organisation's department of learning and development retains training evidences carried out for all its staff members. As part of induction training and ISMS awareness training, staff members must be constantly reminded of the policies related to information security and its objectives. Role-based training must be given to the staff members to enhance the efficiency of ISMS. Managers must review their teams' compulsory training records at any moment. Management emphasises the significance of staff involvement for the efficacy of ISMS implementation and the improvement of security procedures and controls.

The information security department must plan for broad information security related communications throughout the organisation. The internal communication needs are identified in conjunction with the ISMS definition. It includes critical process-related communication requirements, such as what to communicate, when, with whom and how to communicate. The Business Continuity Plan includes communication requirements that influence regular company activities during disasters.

5.4 IDENTIFY THE PRIVACY BY DESIGN APPROACHES

As described in the case study design, once the awareness is created of privacy and security requirements for an organisation, the task of implementing technical solutions is undertaken. Based on the assets identified and the associated risks involved with those information assets, a database management system was used to pseudonymise the data set that was considered for the study. Also, a software utility tool was developed for the same purpose. Following is the analysis of the approach followed in implementing the solution for the case study.

The rationale of Privacy by Design (PbD) is strongly linked to Privacy Enhancing Technologies (PETs). PbD is a mechanism that actively incorporates privacy policies straight into IT, corporate policies, physical design and interconnected technology, which renders protection by default. PbD helps determine data protection requirements across the phase of system implementation, from concept to deployment. Described here are PbD's seven basic concepts. 1) Proactive rather than reactive: Getting all policies related to privacy and procedures primed proactively prior to any privacy events take place. 2) Privacy as the default: Have distinct guidelines for organisation with direct enforcement with policies. These guidelines must clearly state that data will only be acquired and used in a manner that respects individual demands and protects private data. 3) Embedding privacy into design: The obligation for responsible corporate procedures to incorporate information safeguarding provisions in the design as a component of the data protection policy implementation framework. 4) Full Functionality: Create financial value for organisations that enforce data protection guidelines and strategies whilst also safeguarding the privacy of individuals. 5) Protection of the end-to-end life cycle: Organisations need to establish privacy throughout every phase of the information life cycle, i.e. from original software design before information was even obtained to complete monitoring when information is removed. 6) Transparency and Visibility: Organisations ought to be accessible and provide people with the data they need to be honest and upfront about what they are doing, stand next to their claims and be accountable when issues come up. 7) Respect for User Privacy: Organisations should always acquire, utilise, maintain, distribute and remove data in a way compliant with peoples' privacy perceptions (Gan, Chua & Wong, 2019).

PETs may include privacy as well as security characteristics. Privacy sets out a structure for determining who would have the right to admission and modify private data while security performs those decisions. One of the studies classified PETs into four areas: tools for encryption, tools for policy, tools for filtering, and tools for anonymity. Organisations are using PETs to help comply with information protection laws by enhancing privacy protection of consumers and eliminating unnecessary personal credentials from the transmission chain. Cryptographic PETs assist in protecting the anonymity of users, thus stopping the creation of behavioral profiles and tracking of individuals. Several important cryptographic techniques involve anonymous transmission, group authentication and authentication mechanisms for traits (Gan et al., 2019).

Pseudonymisation can be described as the use of aliases in the method of masking private identities so that information pertaining to them could be treated without realising who the data refers to. It relates to a PET used to remove and replace people's or organisations' real identities. It is helpful in data collection circumstances where big volumes of information are collected from distinct sources for data mining and statistical analysis. Pseudonymisation, unlike straightforward de-identification, allows the correlation of information connected with pseudo-identities. Pseudonymisation is one of the strong and versatile database privacy tools. It protects the identity and privacy of people or organisations and allows information related to pseudo-IDs to be linked (Tinabo, Mtenzi & O'Shea, 2009).

All current methods either mandate that all users share a same master key or depend on a fully trusted service to continuously calculate pseudonyms. The reliability of pseudonyms needed to sustain the usefulness of the data entails intrinsic and serious restrictions on privacy. Pseudonymisation assumes that the transaction materialises in a controlled context, either exclusively at the source of the information or by a specialised organisation within the source trust domain. Pseudonymisation is intended to retain the fundamental usefulness of the information, which is achieved by re-using the same pseudonym for each occurrence of that same unique identifier. This connectivity maintains the vital links between occurrences but is also used for re-identification attacks (Lehmann, 2019).

Encryption is one technique that can provide privacy and confidentiality. Encryption is recognised as one technique that would make sensitive information useless, difficult to read or garbled for unauthorised people. Enforcing and controlling an encryption method needs an awareness of fundamental encryption procedures, knowledge of the security features supplied by encryption, and understanding of significant specifications for efficient encryption. According to symmetric key encryption, the encryption mechanism converts the clear text into ciphertext and undoes the ciphertext to its initial form for the decryption mechanism; the encrypting and decrypting mechanisms essentially share the same cryptographic key (Stine & Dang, 2011). The key selection in cryptography is essential because it relies entirely on the protection of the encryption algorithm. The effectiveness of the encryption algorithm depends on the key's secrecy, key length, initialisation vector and how all of them function together (Kurniawan & Munir, 2016).

Requirement processes of engineering are using different ideas to create and model technical and operational requirements. Owing to the large number of occurrences of privacy breaches, enhanced customer perception of privacy, a prevalent knowledge that privacy is a broad-faceted notion which needs emphasis from the initial phases of the design of framework. Several software development techniques have been implemented and current techniques have embraced their operational techniques so that data protection specifications could be established and implemented. As IT is growing quickly, developers are designing mechanisms that use various technologies and resources to satisfy prospective customers. It would be worth noting that a model can be used if consumers both with and without technical know-how can utilise the model and achieve their goals without the expertise of the mechanisms of the core framework. Usability is crucial in IT industry, as any technology must be used to assist customers in the successful completion of their responsibilities. Usability is evaluated through the UI and the system. Usability requirements can be regarded as a basis for software developers designing applications to assess the system's usability on time. Usefulness, effectiveness and fulfilment are three conditions that must be met by a system according to ISO 9241-11. In addition, other studies have revealed that apart from these three criteria, there are other criteria too which must be considered while designing a useful system. Most popular criteria recognised are: convenience, ability to adapt, look and feel, completeness, consistency, customisation of controls, error avoidance, support, learning, memorability, predictability, reliability, responsiveness, simplicity, clarity, user friendliness, usefulness, value and visibility (Pattakou et al., 2018).

As part of the case study, it was demonstrated that the efficient usage of database management tool, such as the Microsoft SQL Server Express 2017, can achieve the cryptographic control implementation for securing the personal information. The software utility tool provides a handy solution to those organisations who are extensively dependent on MS Excel based applications. The case study also demonstrates the benefit of combining both the database management tool and the in-house developed software utility tool to achieve a more robust security mechanism, which in-turn is used to ensure privacy of the data subjects.

5.5 COLLECTING, PROCESSING AND SECURING THE PERSONAL INFORMATION

As described in the Chapters 2 and 3, collecting and processing of private data is restricted and controlled to a great extent. The information assets considered for this study are secondary publicly available data sets. Two publicly available data sets were identified and selected for the study. From the analysis below the evaluation criteria to be followed to comply with the GDPR are identified.

Personal Information (PI) is the information which could be made use of alone or in combination with other information to detect, interact or trace a sole individual, even if the person is not clearly identified by the information alone. The following is an illustrative example of data components that may be a PI by itself or along with other personal information and used to identify an individual: bank account data, beneficiaries, biometric records, birthplace, bonus, / perks, country, state or town of residence, credit card numbers, criminal record, date of birth, digital identity, driver's license number, history of education, email address, emergency contacts, employee ID, ethnicity, financial information and accounts, fingerprints, full name, gender, genetic information, health information (including conditions, treatment and payment), health care providers and plans, telephone numbers, IP address, job title, login name, MAC address, marital status, military rank, mother's name, national identification number, passport number, performance assessment, photographic images, PIN, political affiliations, information about property, religion, wages, screen name, sexual orientation, social security number, taxpayer information, membership of the Union, registration number of the vehicle, and so on.

Privacy will become a commercial variable as collecting information and processing strategies begin to differ significantly throughout the industry or between the customers who do business with the same organisation. It does seem feasible that businesses can transform their design for privacy into a strategic advantage by catering to the requirements of their users by implementing a superior design than their rivals, and thereby might obtain greater share of the market or greater income per client. It is not really a straightforward job to produce an ideal privacy design that benefits both the business and its clients. However, one basic assumption for making privacy a unique selling point is whether the customer knows it, acknowledges it and thinks that the potential advantages are significant. Past consumer research established the understanding of privacy as a 'satisfier'; where clients will appreciate elevated performance, but bad performance might not be penalised (Preibusch et al., 2013).

There is a strong value for the information privacy among the population at large and customers are worried about how well their private data is secured. Just a limited percentage of users opt against their will to share information. Businesses avoid trying to scare off three-quarters of their prospective clients if unreasonable information collection is carried out. Most of these unhappy clients will move to a rival company. When this choice is not available, the business will be discontinued, or incorrect information will be supplied. In fact, supplying incorrect data is a prevalent approach for mitigating the danger of privacy or avoiding excessive spams (Preibusch et al., 2013).

The conventional lawful way to protect privacy is inadequate. As commonly recognised by academicians of privacy law, privacy violation is divided into four classifications: 1) solitude disruption, 2) causing embarrassment by public revelation of personal information, 3) promoting negative opinion, and 4) name or description erasure. As many researchers have pointed out, the law on privacy in this information age is becoming useless in redressing the collection, use and disclosure of private data. Privacy law has significant online intimidation constraints. The primary reason why privacy legislations are ineffective is that the danger associated with collecting, using and distributing private information is exponential. In a single act of collecting, using and distributing private information, there is generally no distinguishable danger (Xiaodong, 2018).

The enormous amount of financial losses owing to private data leaks and spam messages shows the present condition of revelation of private data and causes problems among individuals. There are two most notable issues in this information age: The first is that private data collection sources are much more diverse, such as internet browsing patterns, spending patterns, social media, etc. The second is that private data collectors are more complex. In the earlier data collection method, there was a direct correlation between both the data collector and the data provider, however in the digital age, such a direct link is interrupted by the defensive and offensive coalition and the exchanging of benefits among the data collectors. Data collectors can share private data with the other partners and receive identical data from them, making it hard to track the right to protect private data. The public authorities could also unconditionally obtain private data based on safety of the public or state security and subvert the validity of the authority to private data (Hanlin, 2018).

Accountability and business evaluation are very essential for managing private data misuse. In several instances, the breach of private data is not the general behavior of business policymakers, but the data that staff members have stolen because of their own agendas. Thus, if we could just reinforce the monitoring and training of individuals responsible for the appropriate data, we can to some degree at least decrease the breach of the right to private data. At the very same moment, we could link to private industry private loan documents and blacklists to create company credit reports and blacklists. Any organisation that breaches or wrongly utilises private data would be registered in the blacklist. In addition, the existing unwanted collaboration of the defensive and offensive coalition or the transfer of data needs to be modified to a fresh state of collective monitoring. By establishing a sequence of mechanisms of rewards and punishments, like Penalising irresponsible businesses and compensate the businesses that report data misuse. Private sector undertakings can voluntarily take the lead to undertake collective monitoring, which would significantly decrease the cost of government monitoring and, at the same time, boost general monitoring severity (Hanlin, 2018).

For people, violating the authority to private information is not, for the most part, an individual responsibility or error. Conversely, in several instances it is hard to turn down the collection of private data by the people themselves. As in many instances, even without the involvement of appropriate people, the right to personal data is infringed. Hence it is acknowledged that reducing private data breach by enhancing information security understanding and computer awareness will have little impact. Likewise, for modern technology, data breach is often unrelated to technology. It is a human issue. Regardless of how much technology is improving, it is not possible to mitigate people in charge of themselves. In most occasions, local area networks within organisations have a big quantity of private data. It is very hard for external exploits. Therefore, the security of personal data by technological advancements could only be confined to some degree in order to safeguard the data that hackers illegally seized (Hanlin, 2018).

Hence from the case study it is concluded that, to be compliant with GDPR, there must be a multi-dimensional approach adopted by organisations to secure the information collected by organisations. The personal information collected by organisations can be those that belong to the customers who has business interaction with the organisation, or that of the employees of that same organisation. In either case, organisations must ensure privacy and security of all the personal information that it collects and maintains. As the information collected would correspond to the EU data subjects, and businesses globally are mandated to follow the GDPR directly or indirectly. It would not be a feasible solution for businesses to segregate the information of EU data subjects and adopt privacy and security measures as expected by GDPR, and not to adopt the similar mechanisms for non-EU citizens.

Organisations must collect and process information in a legal, impartial and crystal-clear manner. The motive of the data collected must be made known to the citizens clearly. The information collected must be at minimum such that only the data required by the organisation for a specific purpose alone is used for processing. As excessive information gathered could be made use for other motives, the purpose limitation will confirm that the information is not misused. The information gathered must also be accurate as processing of the data collected would be reliant on the data accuracy. If the information collected is not accurate, it must be discarded or updated with the accurate information. The information collected must not be retained for an indefinite period. Data retention period must be defined for all the types of information collected. Based the data retention period, when the appropriate information completes its retention period, it must be deleted from the organisation's database. Finally, organisations should confirm the concealment and veracity of the data collected. It must be ensured throughout the data lifespan.

From the case study it is also evident that by adopting Privacy Enhancing Technologies, the rights of the citizens would be upheld. Through the usage of the right technology, the data subject would be made available with access rights to the information gathered by the organisation. This information will be made available to the citizens in plain text format. But within the organisation, such information shall be pseudonymised and stored securely. The use of the technologies also enables the data subjects to rectify the information that had been shared at some point of time. If the data subjects wish to not continue their association or service from one of the organisations, they may request for deleting the information collected. By adopting adequate technologies, organisations can remove the information as requested by the data subjects. These technologies also allow to keep a trace of all the information collected within the organisation. By enabling traceability, the processing restriction could also be achieved, which also happens to be one of the rights of the citizen. By using the pseudonymisation technique, it allows the data portability right of the citizen to be implemented judiciously. The transfer of data could occur within the EU or with the notified adequate countries. Pseudonymisation allows the transference of information in a protected way. By enabling the traceability function, the citizens would have the authority to object the processing of data. The processing could be objected up to the extent of automated decision making, which includes profiling by the organisations.

5.6 FUTURE WORK

The risk assessment performed as part of the case study is limited to the representative risks identified in an organisation. The risk assessment can be done in a detailed manner which includes quantitative mechanisms. This would ideally include the association of numerical values to the impact, threats and vulnerabilities. The numerical value derived would provide the perception if the risk is possible to occur or not. Further, based on the quantitative analysis, the risk mitigation, contingency and treatment could be performed. The output from such a detailed analysis would be of immense help to organisations. Also, enough attention should be adopted to confirm that the risks identified are not revealed among the staff members and that it must be limited to the personnel concerned on a need to know basis.

The role of Human Resource (HR) department of an organisation is vital to ensure security and privacy. The HR department’s involvement in handling such activities would be crucial in achieving the management’s security and privacy objectives. A very detailed framework for imparting awareness and training to staff members of the organisation is a necessity. The awareness and training initiative must include a host of components to increase awareness including promotional events and the disbursement of brochures or blog posts. The training in awareness could use various deployment tools, such as in-class, remote teaching, via the internet, self-study, and so on.

The protection of the encryption relies on the cryptographic key's secrecy. All individuals and systems that are not permitted to see the clear text must kept away from accessing the cryptographic key. Even though a powerful cryptographic key is developed yet not held confidential, the information will no longer be secured. The cryptographic key must always be secured against alteration. The clear text cannot be regenerated if the cryptographic key is altered. Cryptographic keys may be altered deliberately or inadvertently. The clear text (secured information) is destroyed when it occurs. Systems that uses encryption must have a procedure for recovering the cryptographic key if it is destroyed or altered (Stine & Dang, 2011). The cryptographic key management could be one of the future studies where the entire lifecycle such as creation, saving, retaining, accessing, sharing, withdrawing and disposal of the keys be presented as a case study.

Chapter 6
CONCLUSION

Data privacy relates to the inalienable right of a person to regulate how any other institution collects, processes, distributes, shares and uses private data. Owing to the interference of social networking sites and the rapid growth of fresh online engagement techniques, the threat of data privacy has already risen. Extensively, private information of people is included in the basic resources for most personal communications, with one another, with firmly entrenched societies and with regulatory officials. In addition to the advantages of state involvement in decision-making mechanisms, such changes are followed by privacy threats that may adversely affect the involvement of individuals. The GDPR is particularly appropriate in this regard (Diamantopoulou et al., 2013).

Organisations must implement the GDPR in order to achieve their business objectives. There is a strong necessity to highlight its advantages for organisations and the principles that contribute to the company's success. Comprehending the GDPR as one more limitation to a business success is incorrect. GDPR is an instrument for creating a practical benefit centered on confidence between the organisation, its staff, customers and associates (Lopes et al., 2019).

For several years, the EU and the U.S. data privacy regulations depended on definitional distinguishing to prioritise legal rights, responsibilities and limitations on data processing operations. Predicated on the belief that sensitive information in existence continues to be positively correlated with higher risks, then information classification continues to be at the center of both continents' privacy regulations. Presently, the extent of information classification is steadily declining since the long-standing differentiation among delicate and insensitive information, has always been questioned (Fazlioglu, 2019).

Organisations must enforce security standards to ensure that the public service is sustainable and that its data is protected. They must establish more comprehensive information security policies that each area of interest demands, and regularly assess them. This approach should be implemented by recognising possible risks for all assets, including staff members. Establish an information security awareness program for staff members and track enforcement. ISA's potential attention can be assigned to awareness-based programs to have a noteworthy effect on the behavior and actions of staff members. Socialising about data security tasks and duties, with internal staff members is necessary.

The following variables require periodic ISA measurements for staff members: new staff members joining each year, global trends in information technology, social relations; and assess the conformity of their staff members about information security (Wahyudiwan et al., 2017).

Every stakeholder needs to build up a progressively elaborate awareness of the realistic and legal circumstances, when considering appointing, perusing and utilising Privacy Impact Assessment records. PIA has capability as a confidentiality assurance method, however that capability may be acknowledged when it is recognised that a PIA statement is not a culmination and does not steer independently to improved confidentiality results. Advisors completing PIAs work under huge restrictions and are put through substantial pressure that may keep them from accomplishing the procedures and reports as anticipated by others. PIA can at any rate give valuable data to others to design projects, make decisions and implementation strategies (Waters, 2012).

The concepts of Privacy by Design (PbD) calls for constructive privacy attention from the beginning of an assignment. Such a strategy has been publicly adopted by Data Protection Authorities, which are legitimately needed by GDPR and endorsed by the European Commission to promote the information-based system. For the PbD to really be feasible, specialists need to participate efficiently in the system because they are eventually accountable for developing their solutions. If not, PbD risks to becoming a meaningless acronym, and a concept with little or no true effect. PbD has so far not achieved extensive and effective acceptance in engineering owing to a discrepancy around legal and technical understanding. According to the standpoint of engineers, confidentiality is generally regarded solely from the view of data protection; and confidentiality and information safeguard appear to be ignored in terms of technical models and design, rather depending on adherence to privacy policies (Martin & Kung, 2018).

Software solutions for privacy governance strive to simplify the process of unconventional adherence with privacy laws such as GDPR. Such techniques always address non-engineering accounts and are separated from software development procedures. The office of legal privacy is address by the Privacy Program Management (PPM) solutions and the IT departments are addressed by Privacy Enterprise Management (PEM) solutions. These solutions are again intended to play a supportive role for the legal departments. Such techniques would not therefore be incorporated into the development cycle of engineering. Programmers and technicians consider privacy and information security unrelated to their job and, most significantly, adopt privacy management techniques instead of engineering practices (Martin & Kung, 2018).

A multitude of alternatives had already been explored and developed from the solely technical sphere to generate privacy-enhancing technologies (PETs) to address the apprehensions related to privacy. Privacy-Enhancing Technologies to most technicians stay unfamiliar owing to the separation of PETs and the method of organic nature of technology and growth, that results in technicians becoming ignorant or uncertain of the adequacy of such alternatives. If technicians encounter concerns about privacy, they use tailor-made alternatives instead of selecting the comprehensive and cost-effective implementation of existing state of the art alternatives (Martin & Kung, 2018).

The PETs had varying consequences on the volume of work of the staff members, the time necessary to perform the job and the pressure of information sharing depending on the nature of their job. Also, it was discovered that PETs implemented more comprehensive and consistent working practices to safeguard private information while acknowledging the need for efficient measures to regulate human elements and risks. The quantity of private information gathered by organisations will rise with growing online footprints. Organisations have a duty to safeguard the interests of their customers by improving the efficiency of their PET services, establishing efficient processes for managing access to private information of customers and increasing awareness of privacy protection and compliance among employees. Public authorities and legislators must also develop efficient supervision strategies to assure organisational compliance with privacy laws in order to safeguard their citizens' privacy (Gan et al., 2019).

Given the latest GDPR legislation, the preservation of the privacy of individuals is an exceptionally significant element of online activities, in which distinct interested parties express notions and stances on policies-related issues. Privacy is generally regarded as an unwelcome distraction throughout the development of products and services that support privacy preservation techniques owing to the absence of software architects and developers' knowledge. Throughout the earlier chapters, approaches to crowdsourcing were analysed with a thought to the data privacy of individuals producing data in the assets they were using. The assessment disclosed helpful understandings into the difficulties posed by various types of crowdsourcing to private information and privacy. While the primary criteria, notably validation and approval, as well as pseudonymisation, were met for both expert-sourcing and citizen-sourcing traditions, obscurity, unlinkabililty, undetectability and unobservability were either breached or not guaranteed (Diamantopoulou et al., 2013).

The study findings indicate that the overall interest in information security is only mildly helpful in anticipating business decisions in a global environment. Users opt for a hostile company against their privacy alternatives, if a cost reduction could be obtained. But their activities are evidently not compatible with the approaches to privacy. An overall inability to see business judgements guided by a specific company privacy design should not be linked to an excessively high price gap, a materialistic attitude, a carelessness in assessing substitutes or overall trust impacts. Users that are more associated with privacy generally display a business decision that more strongly corresponds to their expectations. Competition on privacy is not futile and concluding that the privacy-friendly company is, wholeheartedly, the victim might be incorrect. (Preibusch et al., 2013).

Through the case study demonstration, it is observed that by securing the legacy dataset, an organisation can conform to the GDPR. The demonstration through this case study might be of a smaller scale. But the methodology adopted in cleansing the legacy dataset to comply with GDPR would remain the same across most of the organisations. The case study was initiated with the brief review of the GDPR requirements. It is to be noted that when an organisation has an objective for privacy and security, the implementation of good practices through the known standards is inevitable. Similarly, the case study has demonstrated the benefits of applying the combination of ISO 27001, ISO 31000 and BS 10012 standards. The adoption of these practices allows an organisation to collect and process any personal information in a secure manner. The implementation of PET through PbD was demonstrated by using a database management tool and a cryptographic software utility tool.

The insights that can be extracted from the case study are multi-dimensional. The organisations would have changed their entire mindset to a privacy aware culture. All the issues related to privacy that at some point would have impacted the organisation’s objectives to adhere with the GDPR. It begins with the identification of all the stakeholders and the corresponding necessities in meeting their privacy obligations. Based on it, the applicable management strategies are defined and finalised. The management shall formulate all the necessary policies. If existing policies are available, they shall be reviewed to accommodate the GDPR requirements. The roles and responsibilities as required under organisation’s requirements shall be implemented in this regard. This in turn enables the management to inculcate a privacy-aware culture within the organisation.

From the risks identified, it is observed that the assessment provided an assurance to achieve the privacy objectives of an organisation. It enables in deciding the reduction, avoidance, transference and acceptance strategies for the risks identified. Through a continual process, risks must be reviewed, and new risks must be identified. The management must also ensure that the risks identified would also pose a threat to the organisation as they can be used as vulnerabilities to create malicious activities. The access control mechanism to all such records and tools must be in accordance with the data classification guidelines drafted by the organisation. The impact from risks to the organisation would not only be focused on privacy, but the impact on financial implications to an organisation due to the privacy breach. The risk prioritisation must be focused on the penalties that the organisations may face due to the breach in privacy. The training and awareness programs must focus on such elements to sensitise the staff members on the possible legal implications that the organisation would face in the case of a breach. The awareness programs must be performed periodically, rather than as a one-off.

The management must also decide on the utilisation of cryptographic techniques to safeguard confidentiality, integrity and availability of the information. Most of the applications and services are secured through the implementation of cryptographic controls. Similarly, the personal data collected by the organisation too could be secured through cryptographic controls. In the case study, it was demonstrated by using the database management tool and a software utility tool. The cryptographic technique used in both the methods was symmetric encryption. The key management for such cryptographic controls would be a challenge and hence must be founded on a strictly needs to know basis.

The monitoring and continual improvement of the implemented strategies is a crucial element to achieve GDPR compliance. Internal audits and spot checks could assist in ensuring the security and privacy objectives of the organisation. Such measures ensure that the strategies identified through various policies are enforced and followed by all the stakeholders. All deviations must be analysed thoroughly to identify the root cause. If the cause is a system-wide issue, then the policies must be revisited to incorporate necessary changes to be compliant with GDPR.

To summarise, the research question was to identify the possible ways by an organisation to comply with the GDPR with respect to the legacy data-sets collected. Accordingly, the case study objective of this thesis was achieved by demonstrating the usage and implementation of international management and technical standards to secure the data collected by an organisation to comply with the GDPR.

Finally, the following are the areas for further study and exploration:

1) The implications of GDPR varies from country to country. Hence the redressal of adhering to the legislation could vary from region to region. A study could be conducted on this area drawing the challenges in adequate and non-adequate countries as identified in the GDPR.
2) The implementation of GDPR from management standards perspective is a potential area for learning. The certification of organisations for GDPR compliance is at a very nascent stage. Hence this area could be explored.
3) Privacy has had a major cultural impact on organisations that were lenient on implementing or addressing the related risks. Organisations that followed a security-aware culture would have less impact. Whereas, for organisations which never had any controls to ensure privacy or security would face internal conflicts or push-back. This could be an area of future study.
4) The identification of technological controls to ensure privacy could be another area of focus. Tools that could ensure data collection minimisation within organisations could assist in this area. When the collected data is minimal, the risk to organisation also reduces.
5) There are a certain number of countries / regions which do not possess privacy related laws. Data collection and processing is done vaguely with no regards to impact on privacy. A study could be performed on the awareness level from the general public perspective to learn their opinion.

REFERENCES

Agrawal, V. (2017). A Framework for the Information Classification in ISO 27005 Standard. (2017). IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, 264-269. https://doi.org/10.1109/CSCloud.2017.13

Atkinson, L. (2018). Interpreting the child-related provisions of the GDPR. Communications Law, 23(1), 31-32. Retrieved from https://bloomsburyprofessionallaw.com/looseleaf-journal/communications-law/

Astrup, J. (2018). GDPR: The Transfer of Data Power. Community Practitioner, 91(5), 36–39. Retrieved from https://www.communitypractitioner.co.uk/features/2018/06/gdpr-transfer-data-power

Azzi, A. (2018). The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, (2), 126-137. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/jipitec9&div=15

Bennett, B. (2018). The new rules on customer data and privacy. NZ Business. 32. 46-47. Retrieved from http://ndhadeliver.natlib.govt.nz/delivery/DeliveryManagerServlet?dps_pid=IE37690627

Bhatia, J., & Breaux, T. D. (2018). Empirical Measurement of Perceived Privacy Risk. ACM Transactions on Computer-Human Interaction (TOCHI), 25(6). https://doi.org/10.1145/3267808

Blair, B. T. (2018). Seven Key Concepts Organisations are Getting Wrong About the Global Privacy Law. Journal of AHIMA, 89(6), 44–64. Retrieved from https://journal.ahima.org/2018/06/01/june-2018/

Bowen, R. (2018). GDPR compliance: How to make sure your organisation is prepared. Briefings on HIPAA, 18(2), 5–7. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=ccm&AN=127837765&site=eds-live

BS 10012:2017+A1:2018 Data protection. Specification for a personal information management system. (2018). BSI Standards Limited. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edsbsi&AN=edsbsi.30378574&site=eds-live

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. Information and Communications Technology Law, 26(3), 213–228. https://doi.org/10.1080/13600834.2017.1330740

Burns, S. (2018). GDPR Compliance: The Devil Is in the Details. Computer Weekly, 27-29. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=130250083&site=eds-live

Calder, A. (2018). EU GDPR: A Pocket Guide (European second edition). IT Governance Publishing. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cat05020a&AN=aut.b26123666&site=eds-live

Chirica, S. (2017). The Main Novelties and Implications of the New General Data Protection Regulation. Perspectives of Business Law Journal, 6(1), 159-176. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/perbularna6&div=26

City Official's salaries for the City of Phoenix, Arizona. (2015). [Data set]. Retrieved from https://www.phoenixopendata.com/dataset/staff-salaries

Cliza, M.-C., & Spataru-Negura, L.-C. (2018). The General Protection Regulation: What Does the Public Authorities and Bodes Need to Know and to Do? The rise of the data protection officer. Juridical Tribune, 8(2), 489-501. Retrieved from https://doaj.org/article/761000b004e9419fb1a6917156cc13d9

Corner, S. (2018). After 25 years of data protection law, what next? ComputerWorld from IDG. Retrieved from https://www.computerworld.co.nz/article/633578/after-25-years-data-protection-law-what-next/

Cox, S. (2018). GDPR: Don’t Be so Sure It Doesn’t Apply to You. Hospitality Upgrade, 46-48. Retrieved from https://www.hospitalityupgrade.com/_magazine/MagazineArticles/gdpr-dont-be-so-sure-it-doesnt-apply-to-you.asp/

Cvik Eva Daniela, Pelikánová Radka MacGregor, & Malý Michal. (2018). Selected Issues from the Dark Side of the General Data Protection Regulation. Review of Economic Perspectives, (4), 387. https://doi.org/10.2478/revecp-2018-0020

Delgado, C. (2017). Getting started with Steganography (hide information) on Images with C# [Source code]. Retrieved from https://ourcodeworld.com/articles/read/474/getting-started-with-steganography-hide-information-on-images-with-c-sharp

Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S., & Charalabidis, Y. An assessment of privacy preservation in crowdsourcing approaches: Towards GDPR compliance. International Conference on Research Challenges in Information Science, 2018, 1–9. https://doi.org/10.1109/RCIS.2018.8406643

Diver, L., & Schafer, B. (2017). Opening the Black Box: Petri Nets and Privacy by Design. International Review of Law, Computers & Technology, (1), 68. https://doi.org/10.1080/13600869.2017.1275123

Doe, S. (2018). Practical Privacy: Report from the GDPR World. Legal Information Management, (2), 76-79. https://doi.org/10.1017/S1472669618000178

Elkins, S. (2019). Privacy with a European Flair. For the Record, 31(3), 18–21. Retrieved from https://www.fortherecordmag.com/archives/0319p18.shtml

Elluri, L., & Joshi, K. P. (2018). A knowledge representation of cloud data controls for eu gdpr compliance. IEEE World Congress on Services, 2018, 47–48. https://doi.org/10.1109/SERVICES.2018.00036

Elvy, S.-A. (2017). Paying for Privacy and the Personal Data Economy. Columbia Law Review, (6), 1369. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/clr117&i=1437

European Parliament, Council of the European Union. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fazlioglu, M. (2019). Beyond the Nature of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States. Fordham Urban Law Journal, 46(2), 271-306. Retrieved from http://heinonline.org/HOL/Page?handle=hein.journals/frdurb46&div=12

Featherstone, C., & Miller, H. (2018). Why CIOs need to keep privacy front of mind in any project. CIO from IDG. Retrieved from https://www.cio.co.nz/article/641976/privacy-by-design-why-cios-need-keep-privacy-front-mind-any-project/

Gan, M. F., Chua, H. N., & Wong, S. F. (2019). Privacy Enhancing Technologies implementation: An investigation of its impact on work processes and employee perception. Telematics and Informatics, 38, 13–29. https://doi.org/10.1016/j.tele.2019.01.002

Garber, J. (2018). GDPR – compliance nightmare or business opportunity? Computer Fraud and Security, 14–15. https://doi.org/10.1016/S1361-3723(18)30055-1

Ghanbari, E. (2015). Protecting The CDN Application Files From Unauthorised Requests [Source code]. Retrieved from https://www.ehsanghanbari.com/blog/post/186/protecting-the-cdn-application-files-from-unauthorised-requests

Ghosh, D. (2018). How GDPR Will Transform Digital Marketing. Harvard Business Review Digital Articles, 2–4. Retrieved from https://hbr.org/2018/05/how-gdpr-will-transform-digital-marketing

Gil González, E., & de Hert, P. (2019). Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. ERA Forum, 19(4), 597-621. https://doi.org/10.1007/s12027-018-0546-z

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. 2018 IEEE International Conference on Big Data (Big Data). 5027-5033. https://doi.org/10.1109/BigData.2018.8622621

Gunasekara, G., & Toy, A. (2011). Principles or rules: the place of information privacy law. New Zealand Universities Law Review, 24(1), 525-549. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edsinz&AN=edsinz.997050623602837&site=eds-live

Gundu, T., Flowerday, S., & Renaud, K. (2019). Deliver Security Awareness Training, then Repeat: {Deliver; Measure Efficacy}. Conference on Information Communications Technology and Society (ICTAS), 2019. https://doi.org/10.1109/ICTAS.2019.8703523

Hanlin, D. (2018). The system position and protection of personal information right in general provisions of the civil law. US-China Law Review, 15(3), 150-155. https://doi.org/10.17265/1548-6605/2018.03.004

Hertzberg, J. (2018). GDPR and Internal Audit. Internal Auditor, 75(4), 22–23. Retrieved from https://iaonline.theiia.org/2018/Pages/GDPR-and-Internal-Audit.aspx

Hintze, M. (2018). Data Controllers, Data Processors and the Growing Use of Connected Products in the Enterprise: Managing Risks Understanding Benefits and Complying with the GDPR. Journal of Internet Law, (2), 17. http://dx.doi.org/10.2139/ssrn.3192721

Ingley, C., & Wells, P. (2018). GDPR: Governance Implications for Regimes outside the EU. Proceedings of the European Conference on Management, Leadership & Governance, 105–113. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=133413009&site=eds-live

Jayasinghe, U., Lee, G. M, & MacDermott, A. (2018). Trust-Based Data Controller for Personal Information Management. 2018 International Conference on Innovations in Information Technology (IIT). https://doi.org/10.1109/INNOVATIONS.2018.8605979

John, A. (2018). Utilities sector "among worst" in risking GDPR penalties. Utility Week, 25. Retrieved from https://utilityweek.co.uk/utilities-sector-among-worst-risking-gdpr-penalties/

Kammueller, F. (2018). Formal Modeling and Analysis of Data Protection for GDPR Compliance of IoT Healthcare Systems. IEEE International Conference on Systems, Man, and Cybernetics (SMC), Systems, Man, and Cybernetics (SMC), 2018, 3319-3324. https://doi.org/10.1109/SMC.2018.00562

Kędzior, M. (2019). GDPR and beyond—a year of changes in the data protection landscape of the European Union. ERA Forum, 19(4), 505-509. https://doi.org/10.1007/s12027-019-00549-x

King-Bailey, V. (2018). Mastering EU GDPR Compliance: Security and Privacy for Validated Systems. Journal of Validation Technology, 24(6), 25–33. Retrieved from http://www.ivtnetwork.com/article/mastering-eu-gdpr-compliance-security-and-privacyvalidated-systems

Kurniawan, D. H., & Munir, R. (2016). Double Chaining Algorithm: A secure symmetric-key encryption algorithm. 4th IGNITE Conference and 2016 International Conference on Advanced Informatics: Concepts, Theory and Application, ICAICTA 2016. https://doi.org/10.1109/ICAICTA.2016.7803097

Lehmann, A. (2019). ScrambleDB: Oblivious (Chameleon) Pseudonymisation-as-a-Service. Proceedings on Privacy Enhancing Technologies, (3), 289-309. https://doi.org/10.2478/popets-2019-0048

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. Iberian Conference on Information Systems and Technologies, CISTI, 2019. https://doi.org/10.23919/CISTI.2019.8760937

Ludlam, S. (2018). Drilling for data. Monthly: Australian Politics, Society & Culture, (146), 15–18. Retrieved from https://www.themonthly.com.au/issue/2018/july/1530367200/scott-ludlam/minding-your-data-post-gdpr-world

Martin, Y.-S., & Kung, A. (2018). Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering. 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018, 108–111. https://doi.org/10.1109/EuroSPW.2018.00021

Membrey, D., & Mitchels, B. (2019). Demystifying the General Data Protection Regulation (GDPR): Some of the Issues Relevant to the Counselling Professions. Healthcare Counselling & Psychotherapy Journal, 19(1), 16–21. Retrieved from https://www.bacp.co.uk/bacp-journals/healthcare-counselling-and-psychotherapy-journal/

Mitchell, A. (2016). GDPR: Evolutionary or revolutionary? Journal of Direct, Data and Digital Marketing Practice, 17(4), 217-221. https://doi.org/10.1057/s41263-016-0006-9

Mitchell, M., & Fondi, L. S. (2018). Data Protection Impact Assessments: The European experience. Governance Directions, 70(10), 660–664. Retrieved from https://www.governanceinstitute.com.au/resources/governance-directions/issue-10/data-protection-impact-assessments-the-european-experience/

Ministry of Justice, New Zealand. (1993). Privacy Act 1993. Retrieved from http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

Mueller, B. (2017). GDPR compliance in four steps. LawTalk, (913), 28. Retrieved from http://www.lawsociety.org.nz/__data/assets/pdf_file/0010/117100/913-WEB.pdf

Nasar, M.R.A., Mohd, M. & Ali, N.M. (2011). A conceptual framework for an interactive personal information management system. 2011 International Conference on User Science and Engineering (i-USEr). https://doi.org/10.1109/iUSEr.2011.6150545

Official Journal of the European Union. (2016). Adequacy decisions. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents

Paredes, D. (2019). Accelerating privacy regulation returns as top emerging risk worrying organisations: Gartner. CIO from IDG. Retrieved from https://www.cio.co.nz/article/660122/accelerating-privacy-regulation-returns-top-emerging-risk-worrying-organisations-gartner/

Pattakou, A., Mavroeidi, A., Diamantopoulou, V., Kalloniatis, C., & Gritzalis, S. (2018). Towards the Design of Usable Privacy by Design Methodologies. IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE), 2018. https://doi.org/10.1109/ESPRE.2018.00007

Peltier, T. R. (2014). Information security fundamentals. CRC Press. Retrieved from https://ebookcentral.proquest.com/lib/aut/detail.action?docID=1375200

Preibusch, S., Kübler, D., & Beresford, A. R. (2013). Price versus privacy: an experiment into the competitive advantage of collecting less personal information. Electronic Commerce Research, 13(4), 423–455. https://doi-org.ezproxy.aut.ac.nz/10.1007/s10660-013-9130-3

Puspitaningrum, E. A., Devani, F. T., Putri, V. Q., Hidayanto, A. N., Solikin & Hapsari, I. C. (2018). Measurement of Employee Information Security Awareness: Case Study at A Government Institution. Third International Conference on Informatics and Computing (ICIC), 2018. https://doi.org/10.1109/IAC.2018.8780571

RNGCryptoServiceProvider. (2015). using RNGCryptoServiceProvider to generate random string [Source code]. Retrieved from https://stackoverflow.com/questions/32932679/using-rngcryptoserviceprovider-to-generate-random-string

Ross, J. R. (2019). The Low-Down on GDPR. Successful Meetings, 68(3), 10–12. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=s3h&AN=135517988&site=eds-live

Sari, P. K., & Prasetio, A. (2018). Knowledge sharing and electronic word of mouth to promote information security awareness in social network site. International Workshop on Big Data and Information Security, 2018, 113–117. https://doi.org/10.1109/IWBIS.2017.8275111

Sampat, B., & Prabhakar, B. (2017). Privacy Risks and Security Threats in mHealth Apps. Journal of International Technology & Information Management, 26(4), 126–153. Retrieved from https://iima.org/wp/jitim/

Stine, K., & Dang, Q. (2011). Encryption Basics. Journal of AHIMA, 82(5), 44–47. Retrieved from http://library.ahima.org/doc?oid=104090#.XZSgrkb7TD4

Tankard, C. (2016). What the GDPR means for businesses. Network Security, 2016(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

Tinabo, R., Mtenzi, F., & O'Shea, B. (2009). Anonymisation vs. Pseudonymisation: Which one is most useful for both privacy protection and usefulness of e-healthcare data. International Conference for Internet Technology and Secured Transactions (ICITST), 2009. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edseee&AN=edseee.5402501&site=eds-live

Passenger information from the Titanic. (2015). [Data set]. Retrieved from https://public.opendatasoft.com/explore/dataset/titanic-passengers/information/

Tzolov, T. (2018). One Model for Implementation GDPR Based On ISO Standards. 2018 International Conference on Information Technologies (InfoTech). https://doi.org/10.1109/InfoTech.2018.8510716

Ungureanu, C. T. (2018). Legal Remedies for Personal Data Protection in European Union. Logos Universality Mentality Education Novelty Section: Law, 6(2), 26-47. https://doi.org/10.18662/lumenlaw/10

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective. Journal of Consumer Policy, 42(1), 91–107. https://doi.org/10.1007/s10603-018-9399-7

Vanberg, A. D. (2018). The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience? Journal of Internet Law, 21(7), 1–19. Retrieved from https://arro.anglia.ac.uk/702656/

Wadhwa, K., & Rodrigues, R. (2013). Evaluating privacy impact assessments. Innovation: The European Journal of Social Sciences, 26(1-2), 161–180. https://doi.org/10.1080/13511610.2013.761748

Wahyudiwan, D. D. H., Sucahyo, Y. G., & Gandhi, A. (2017). Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education. 3rd International Conference on Science in Information Technology: Theory and Application of IT for Education, Industry and Society in Big Data Era, ICSITech 2017, 654–658. https://doi.org/10.1109/ICSITech.2017.8257194

Wang, E. S.-T. (2019). Effects of Brand Awareness and Social Norms on User-Perceived Cyber Privacy Risk. International Journal of Electronic Commerce, 23(2), 272–293. https://doi.org/10.1080/10864415.2018.1564553

Waters, N. (2012). Privacy Impact Assessment – Great Potential Not Often Realised. In D. Wright, P. De Hert (eds.), Privacy Impact Assessment, Law, Governance and Technology Series 6. https://doi.org/10.1007/978-94-007-2543-0_6

Wolters, P. T. J. (2017). The security of personal data under the GDPR: a harmonized duty or a shared responsibility? International Data Privacy Law, 7(3), 165. https://doi.org/10.1093/idpl/ipx008

Wolters, P. T. J. (2018). The Control by and Rights of the Data Subject under the GDPR. Journal of Internet Law, 22(1), 1–8. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=131103593&site=eds-live

Wolters, P. T. J. (2019). The Enforcement by the Data Subject under the GDPR. Journal of Internet Law, 22(8), 1–31. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=134619097&site=eds-live

Wright, D., & De Hert, P. (eds.). (2012). Introduction to Privacy Impact Assessment. Privacy Impact Assessment, Law, Governance and Technology Series 6. https://doi.org/10.1007/978-94-007-2543-0_1

Wright, M. T. (2018). What is GDPR, and why should you care? Independent Banker, 68(10), 35–37. Retrieved from https://independentbanker.org/2018/10/what-is-gdpr-and-why-should-you-care/

Xiaodong, D. (2018). Personal data protection: Rethinking the reasons, nature, and legal framework. Frontiers of Law in China, 13(3), 380-389. https://doi.org/10.3868/s050-007-018-0029-6