Universiteit Leiden

ICT in Business and the Public Sector

Data Privacy Transformation – Legislations to Controls

Name: Richard James Hobbs

Student-no: 1227904

Date: 17/09/2020

1st supervisor: Prof. dr. ir. Joost Visser
2nd supervisor: Dr. Cristoph Stettina

Table of Contents

1. ABSTRACT

Background. As the world progresses towards an increasingly digital frontier, individuals are raising concern over the lack of control in terms of their personal data. To protect their citizens' privacy, countries are drafting regulations to provide organisations with specific guidelines on how it is permitted to use an individual's personal data, and the rights an individual has to control their privacy. To an organisation, these regulations are a new challenge. With the regulations being open to interpretation and subject to a grey area over explicit definitions on how to comply, how will an organisation adapt to meet the expectations of individuals while still operating effectively?

Aim. The aim of this thesis is to analyse existing major privacy regulations from around the world to find key similarities in combination with existing information technology frameworks to attempt to bridge the gap in knowledge, understanding, and compliance between legal and IT requirements. This will be achieved by creating a set of operational privacy guidelines, called Privacy Fundamentals, which an organisation can base their privacy compliance on.

Method. We have anlaysed a number of privacy regulations technical (IT) privacy frameworks to find similarities and differences, to observe how these can be related back to a business environment. After finding commonality between legal requirements, and proposals from technical privacy frameworks, a set of controls are to be established, these are then validated by conducting interviews amongst Privacy, IT, and Legal practitioners. Each of the created Privacy Fundamentals will follow the methodology of Design Science in Information Systems Research, with the set of Privacy Fundamental as the resulting Design Artifact.

Results. The analysis of the interview responses show that there is agreement over the requirement to provide a minimum level of information within the Privacy Fundamentals to show what is expected from a stakeholder in order to be compliant with a privacy regulation. The results show that there is also agreement that the proposed reference material within the Fundamentals is a benefit when further explaining the requirement to parties with different knowledge backgrounds.

Conclusion In this thesis we have successfully found a method to provide a set of operational privacy guidelines to an audience with a mixed working background and field of knowledge. These guidelines, or Privacy Fundamentals, provide a clear baseline of what is expected from each stakeholder become compliant to privacy requirements.

2. INTRODUCTION

Since the early 1970s, there has been an ever-growing increase of electronic systems used for the processing of information regarding specific individuals. These systems go back to the humble beginnings where they were classed as electronic record systems, not much more than what could be compared to a library index card system. Initially, within Europe, this was facilitated by the need to share information to allow for uninterrupted trans-border trade, fuelled by the rapid and continuous developments with Information Technology.

In multinational organisations data is a key asset, for most organisations the usage of personal data, data which can us used to specifically identify an individual, is required for operations and to develop future opportunities which may arise with the development of new technology and expanding global markets. The developments offered what could be seen as organisations to be tremendous opportunities and advantages to their overall productivity. As the data collection by organisations increased so did the awareness and concerns of the individuals whose data was collected. Individuals are becoming aware that organisations were often collecting their personal information for purposes unknown to them. The average individual may not have been aware that organisations are transferring, repurposing and even selling personal information to third-parties around the world.

As concerns grew over the processing activities organisations were undertaking with individuals' data, this forced governments at a national level to draft regulations. The regulations were the first attempt to govern how an organisation is required to respect the rights of an individual to privacy. The rights of individuals present significant challenges to an organisation, as the right to privacy is a legally binding requirement in

a growing number of countries and regions around the world, but the overall challenge to comply with this is generally delegated down to the Information Technology departments or organisations within business and enterprises. The translation of legal requirements, being open to interpretation and 'grey areas' leading to incompatibility and misunderstanding with an information technology standpoint where, for the most part, decisions are made on a 'binary level' or defined in black and white with some degree of certainty.

This thesis aims to analyse the legal requirements of privacy laws and regulations from around the world and see how they can fit into an information technology professional understanding and capabilities to ensure the rights and freedoms regarding privacy.

The main focus of the analysis is regarding leading privacy regulations, including the General Data Protection Regulation, the California Consumer Privacy Act, and the Brazilian Data Protection Regulation.

Following the analysis of these regulations, the next task will be to translate the regulations into practical Information Technology requirements, processes, and compliance activities.

In Chapter 3, we will look at existing privacy frameworks which have been written from an IT perspective, in order to gain an understanding as to what has already been attempted, to further analyse how they can be linked back to privacy regulations.

In Chapter 4, the research of this thesis now looks at examples of major privacy regulations to compare and contract any similarities.

In Chapter 5, we focus on combining examples of privacy regulations from around the world to existing privacy (IT) frameworks in an attempt to begin to find an understandable middle ground between two perspectives.

In Chapter 6, we focus upon the implementation of a Privacy Fundamentals Framework for a specific organisation within the logistics industry. This chapter will provide what is expected by an organisation for their employees to ensure their processing activities are compliant to GDPR. The means by which this will be achieved is by conducting interviews with privacy practitioners with both a legal and IT compliance background, and using their experiences to guide the creation of fundamental controls.

2.1 Problem Statement

Information Technology continues to develop new and innovative solutions to improve, automate, and simplify our lives. Everyday paper-based or manual tasks have now matured into what we could deem as either automatic electronic processes or smart systems. Those that have designed in a manner to replace any task or activity that we would have to handle ourselves with somewhat more effort. Even simple tasks such as completing an application form or simply turning on lights have been now matured and enhanced for convenience. Information Technology can inconvenience an individual's rights to privacy. Alan Westin, once described, that there are four states of privacy; solitude, intimacy, anonymity, and reserve (Westin, 1968). The four states describe individuals' expectations in terms of privacy and how computer systems work to achieve this.

Innovation in information technology occurs consistently and aims to provide an improvement or enhancement to our lives. These technologies themselves come at what we could define as a cost to an individual's privacy. A primary and somewhat early example of this is a loyalty scheme for a store. There is a cost/benefit relationship to both parties, the organisation and the individual, both sides benefit. However, there is a cost to each party for the benefit to the other.

The challenges now are to develop systems which have both parties' best interests at their core, the Privacy-by Design methodology. In contrast, enterprise systems aim to improve organisational processes. As privacy regulations have matured there are now requirements on information technology professionals to develops systems which are not privacy-intrusive. Systems which are non-privacy intrusive can be challenging to balance within an enterprise situation as the rights of individuals must be balanced against the overall business requirements and goals of efficiency, growth, and profits.

An additional challenge to organisations is that they also need to analyse their existing systems and processing activities to ensure they are compliant with modern privacy requirements. An example of this would be when looking at a marketing system, would a system developed internally for a marketing activity can fulfil the requirements in place for Data Subject Access Requests, the ability to remove, amend, or opt-out of being processed.

2.2 Research Question

The research question posed by this thesis is:

How can privacy regulations be translated into meaningful guidelines for information technology professionals to implement?

2.3 Research Methodology

In this master thesis we provide an analysis of the legal regulations regarding an individual's rights and freedoms to privacy, as they relate to business information systems. This analysis will look into what this means to an organisation in terms of impact and changes to processing behaviour, and how these legal requirements will

translate into meaningful guidelines for the information technology professional to implement.

For this thesis, a qualitative methodology is used to provide a comparative study into how the major privacy regulations globally can be analysed and combined with information technology best practices in the field of information technology. The study will consist mainly of literature reviews of regulations and frameworks, and a narrative methodology based on the researcher's own working experiences within the field of privacy.

The research into the subject is conducted using the published guidelines for the privacy regulations around the world, namely the:

- European Union's General Data Protection Regulation (GDPR);
- California Consumer Privacy Act (CCPA);
- Brazil's General Data Protection Law (LGPD).

For Information Technology practices, further analysis will be performed on frameworks such as:

- The Fair Information Practice Principles (FIPPs) published by the Federal Trade Commission (FTC) (1977);
- The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data published by the Organisation for Economic Cooperation and Development (OECD) (1980);
- NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management published by the National Institute of Standards and Technology (NIST) (2020)

2.4 Research Context

For this thesis I will be drawing upon my own experiences within the field of Privacy for a global logistics organisation as a privacy practitioner. I believe my experiences and background are suitable for this researched based on my total number of years working experience and the certifications I have gained during this time, namely:

- IAPP - Certified Information Privacy Professional / Europe (CIPP/e)
- IAPP - Certified Information Privacy Manager (CIPM)
- IAPP - Fellow of Information Privacy (FIP)
- ISACA - Certified Data Privacy Solutions Engineer (CDPSE)
- OneTrust - Fellow of Privacy Technology (FPT)

2.5 Design Science

Information systems and organisations that support them, are complex, artificial, and purposefully designed. They are composed of people, structure, and technology (Hevner, March, Park, & Sudha, 2004). When implementing an information system within an organization, the organization will analyse the effectiveness and efficiencies that are expected for a new system. The capabilities of a new information system are defined by its: People, Development, and Implementation (Silver, Markus, & Beath, 1995).

In figure 1, we see an overview of how a business' strategy provides guidance, or requirements, to the information technology strategy of the organisation. Once the strategies have been defined both the information systems infrastructure and the resulting organisational infrastructure can then be defined and implemented. The

resulting organisations infrastructure can then guide the future business strategy of an organisation.

FIGURE 1 ORGANISATIONAL DESIGN AND INFORMATION SYSTEMS DESIGN ACTIVITIES (ADAPTED FROM J.HENDERSON AND N. VENKATRAMAN) IBM SYSTEMS JOURNAL 1993

Henderson and Venkatraman show that the translation of strategies to infrastructure requires input from both sides of the cycle. Organisational strategy is used to create organizational infrastructure overall, and the organisations strategy inputs into the information strategy to create the supporting information systems infrastructure. Whilst all of these are independent of each other, the common ground between these is that information technology and systems are seen as a compliment, or enabler of organization infrastructure and business strategy. Zmud states that knowledge regarding the use of information technology and the usage of information technology for managerial and organizational purposes is also required to aid the application of information systems to human organisations (Zmud, June 1997).

In order to acquire this knowledge, March and Smith argue that "two complementary but distinct paradigms, behavioural science and design science" bust be explored (March & Smith, 1995).

Behavioural Science originates in natural science research, it exists to "develop and justify theories that explain or predict organizational or human phenomena surrounding the analysis, design, implementation, management, and use of Information Systems" (Hevner, March, Park, & Sudha, 2004).

Behavioural Science theories inform researchers, organisations, and practitioners of the interactions between, people, the organisation, and information systems, and how they will be used to achieve their intended purposes. The purpose effectiveness is impacted by the design science or decisions made when developing an information system, in terms of capabilities, contents, and interfaces.

Design Science originates from engineering and artificial sciences. As a problem solving paradigm it "seeks to create innovations that define the ideas, practices, technical capabilities, and products which the analysis, design, implementation, management, and use of Information Systems can be effectively and efficiently accomplished" (Denning, 1997) (Tsichritzis, 1998).

In similarity with Behaviour Science, Design Science required reflection onto "natural laws and behavioural theories" (Hevner, March, Park, & Sudha, 2004). The Design Science theories are applied, tested, modified, and extended through experience, intuition, and problem solving capabilities (Markus, Majchrzak, & Gasser, 2002) (Walls, Widmeyer, & El Sawry, 1992).

Hevner, March, Park, and Ram present a conceptual framework for understanding, executing, and evaluating information systems research combining both behavioural science and design science paradigms (Hevner, March, Park, & Sudha, 2004).

The framework, as shown in Figure 2, divides research into Information Systems into three main topics: Environment, Research, Knowledge Base. The environment topic focuses on the goals, tasks, opportunities that define an organisation's needs, it's stakeholders, and the supporting technology. The research topic develops and justify the identified business needs, or artifacts through a continuous process of building, analysing, evaluating, and refinement. Finally, the knowledge base topic focuses on all the key resources, methodologies, foundations, frameworks in which the Research topic is based upon.

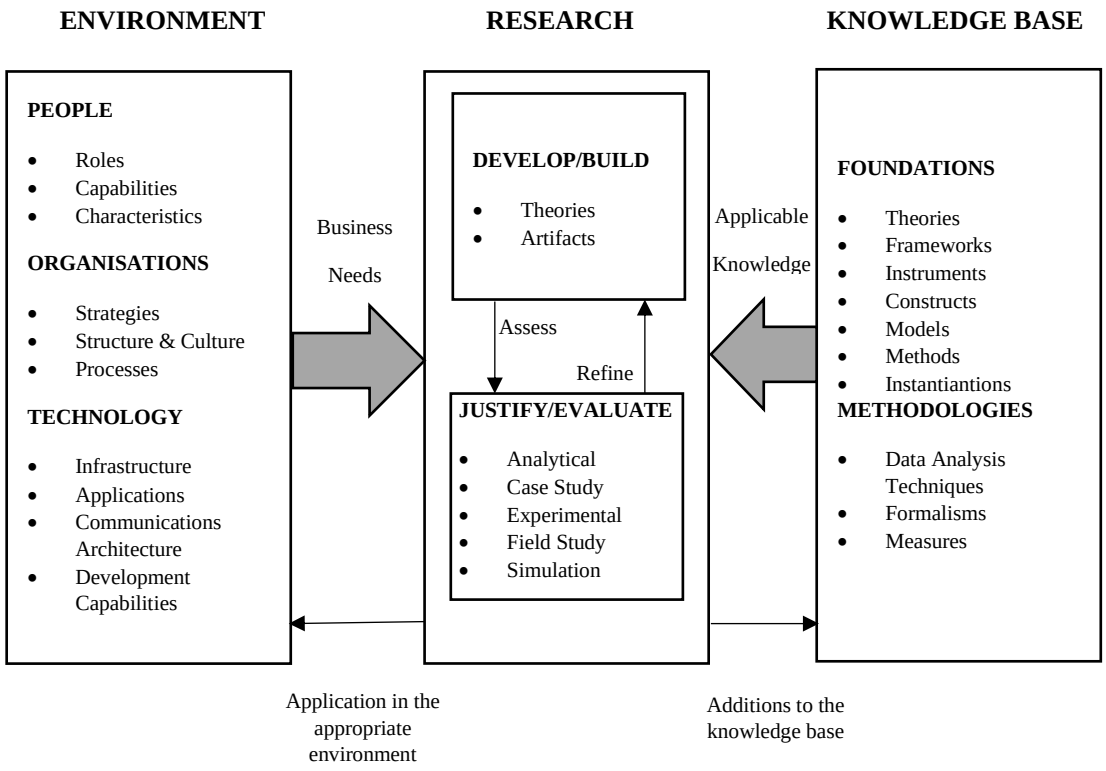


FIGURE 2. INFORMATION SYSTEMS RESEARCH FRAMEWORK - HEVNER ET AL.

Figure 3 shows my own personal interpretation on how the conceptual framework provided by Henver et al can be used for the purposes required by my thesis, to transform the legal requirements into information technology and business artefacts.

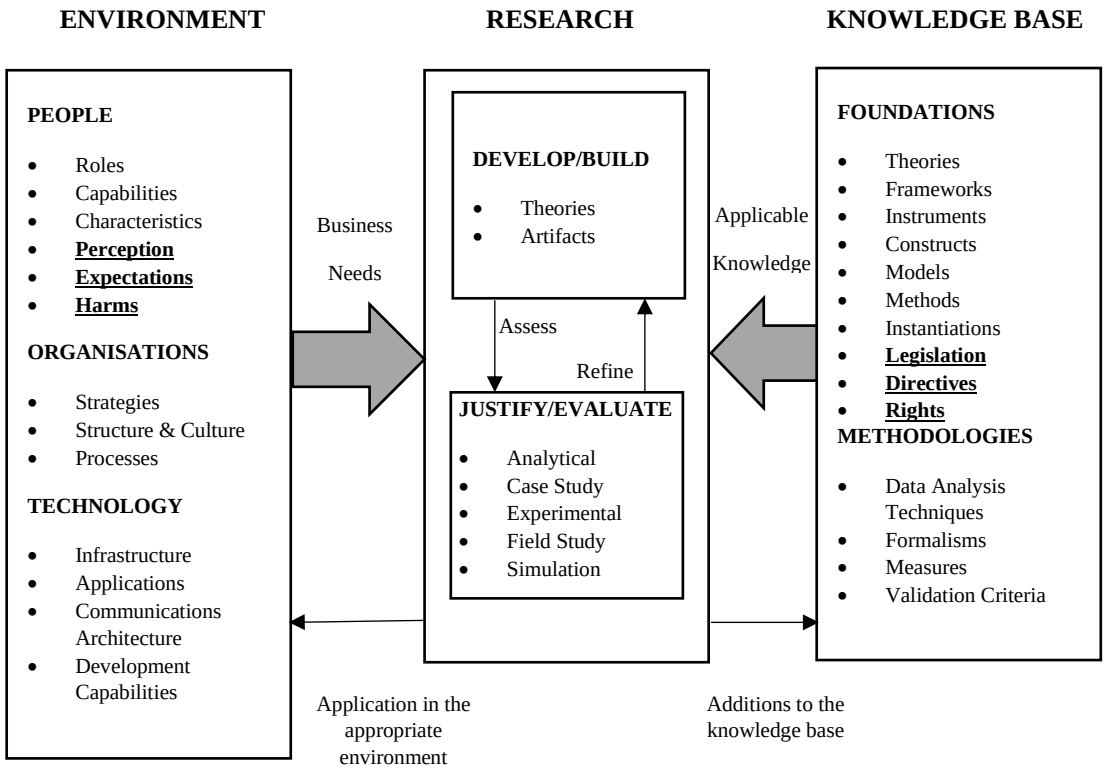


FIGURE 3 INFORMATION SYSTEMS RESEARCH FRAMEWORK MODIFIED

For my interpretation the category of people as part of the environment component has been expanded with three additional topics. The element of perception aims to determine how an individual will perceive any action by an organisation into their personal lives, or even their perception of an organisation as a whole in regard to how intrusive one becomes into the personal lives of individuals. An example of perception in this sense can be that one of two elements, a customer contact form for a simple customer query purpose can be seen as intrusive if additional questions which are perceived as being intrusive and beyond the legitimate requirement. In this case asking gender can be perceived as being intrusive, as an organisation would have to defend

why they need gender as part of their customer support processes. Another example from perception would be in relation to an organisation as a whole, recently companies such as Facebook and Google have been under fire for their privacy practices. Facebook in particular has been part of a number of enforcement cases related to their usage of personal data. This creates a perception with individuals that an organisation has no control over the personal information they have collected from individuals, and seemingly has uncontrollable limits as to what they have decided to do with said information, therefore creating the "they know too much" mindset with individuals.

Expectation, similar to perception, is what an individual expects in regard to both the usage and security of the personal information they have provided to an organisation, and the expectations they may have in regard to their own private life not being subject to interference due to the information they have provided to an organisation. An example of this could be marketing, by providing consent to an organisation to send a weekly newsletter or sales promotion, the individual should therefore expect that their information would only be used for this manner, what does beyond this expectation is the notion that an organisation may pass on an individual's personal information without providing any resulting actions that may occur as a result.

The topic of harms is based upon Ryan Calo's Harm Dimensions, where the harms to an individual's privacy can be split into two types, objective, and subjective. An objective harm is measurable and observable, where a person's privacy has been violated and a direct harm exists. Subjective harms are more in line with perception, where an observable or measurable harm to a person's privacy rights have not been found, but the expectation of a harm still exists. Ultimately these harms have the same impact to an individual, as an individual who expects a harm to occur will take the same action as an individual who has been subject to a harms occurrence. (Ryan Calo, 2010).

2.5.1 Design Science in Information Systems Research

Hevner et al. discus further that as design science is a problem-solving process there are seven guidelines which should apply in order to design a problem and its solution. For the relevance of this thesis, guidelines 1, Design as an Artifact, and guideline 3, Design Evaluation are the most useful.

2.5.1.1 Design as an Artifact

An IT artifact is created to address a particular problem with in an organisation, this could be organisational, infrastructure, or at an implementation level. Hever et al. state that an artifact includes components of the organisation, for example its strategy, and the people involved with the usage of an artifact. They state that "Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation" (Hevner, March, Park, & Sudha, 2004). This is further expanded upon by Denning who states that "artifacts are innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design and implantation and use of information systems can be effectively and efficiently accomplished (Denning, 1997). Simon then states in more simplified terms in regard to the above "solving a problem simply means representing it so as to make the solution transparent" (Simon, 1996).

The artifact I intend to create as a result of this thesis will provide a set of guidelines to both a legal and IT organisation on what is expected of both parties in relation to privacy regulation compliance. These guidelines will provide references to the respective articles within legislation, and information security framework controls to provide a reference to IT professionals when implementing a risk and control compliance program.

2.5.1.2 Design Evaluation

For the evaluation of the created artifact, I will be following the methodology used to [measure] the Degree of Service Orientation in Proprietary SOA Systems (Aldris, Nugroho, Lago, & Visser, 2013). By using this methodology, the Business Requirements (Controls) will be graded on a Likert scale of 1 – 5 based on the following:

- Standardisation
- Abstraction
- Loose Coupling
- Autonomy
- Genericity
- Discoverability
- Composability

3. RELATED WORK

Prior to the start of this thesis, primarily as part of my work within the field of privacy, a number of existing privacy frameworks have been analysed to determine their suitability and applicability to the logistics industry which I am employed within.

The first framework analysed was the TrustArc-Nymity Integrated Privacy Frameworks (TrustArc Nymity, 2020). The approach taken by TrustArc-Nymity is the use of three core pillars to address the main phases of a privacy program, the core pillars are listed as Build, Implement, and Demonstrate. These three cores can be used for both the overall privacy governance of an organisation, or adapted for use within individual compliance activities and processing activities. The content of the three pillars of the TrustArc-Nymity approach can be divided into different business

functions and teams, with the legal teams playing a primary role within most building and maintain tasks, the role of privacy professionals lies within the engage, conduct, and reporting tasks, and finally the IT professionals tasks lie within the implementation tasks. The similarities between this framework and the intended Privacy Fundamental framework is the notion of breaking each legal requirement into a task or responsibility. The reasoning behind why it has been determined that this framework is not adequate for the purpose set out by this thesis relates to the level at which the tasks and responsibilities are written. The high tasks of the TrustArc-Nymity framework provide no detail on what is expected as a result of each requirement.

The next to be analysed was the NOREA Guide Privacy Control Framework (NOREA Guide - Privacy Control Framework, 2018). The objective of the NOREA framework is to provide guidance to professionals to aid the assessment of an organisation's privacy controls and objectives. The primary audience for this framework differs from the intended recipient of this thesis, in that the NOREA framework is more tailored towards audit professionals, and privacy professionals who are focused on gap analysis. The similarities of this related piece are the approach of dividing the main privacy regulations into specific privacy topics and associating the controls to them. The associated controls are written at a level which would be more appropriate to an organisation as a whole instead of a processing activity.

4. TECHNOLOGY STANDARD FRAMEWORKS

The development of technology standards for privacy by information technology professionals was in 1972. The first example of privacy standards in the United States were created by the Health, Education and Welfare Advisory Committee on Automated Data Systems; these are known as the Fair Information Practices (FIP) (U.S Department of Health, Education & Welfare, 1973).

Furthermore, the development of guidelines for Information Technology professionals to adhere to when developing or implementing systems has become more prominent due to the regulations in place to be discussed further in the next chapter.

One major proponent for the development of Privacy Principles or Standards is the Privacy-by-design methodology (Cavoukain & Jones Harbour, 2011) as developed by Ann Cavoukain in 1995. These guidelines aim to instruct developers in the requirements during the design, testing, and implementation of new systems to attempt to preserve the privacy rights of an individual throughout the engineering process.

The basis of privacy-by-design, its foundational principles, have been a critical driver in the direction of most modern approaches to a privacy standard or framework within Information Technology, Table 1 below lists the foundational principles (Cavoukain A. , 2011).

1	Proactive not reactive; preventative not remedial
2	Privacy as the default setting
3	Privacy embedded in the design
4	Full functionality – positive-sum, not zero-sum
5	End-to-end Security – full lifecycle protection

6	Visibility and Transparency – keep it open
7	Respect for user Privacy – keep it user-centric

TABLE 1 - PBD FOUNDATIONAL PRINCIPLES

There have been three significant developments when it comes to trying to standardise the requirements of privacy regulation within Information Technology, and these have all drawn from the recommendations and suggestions from both the Privacy-by-design methodology and the principles as set out by the Fair Information Practices.

3.1 Fair Information Practice Principles

Within the United States, the Federal Trade Commission (FTC) published a set of guidelines to businesses in the United States in 1977, known as the Fair Information Practice Principles (FIPP). FIPPs defined by the FTC are then associated with a specific industries activity and treated with the same fashion as an existing law or regulation. Where applicable, within the US, the FIPP provides a basis of Privacy related legal policies.

As a FIPPs are a high-level definition of the qualities and behaviours expected of a system. Therefore, it is open to interpretation by developers and Information Technology professionals to interpret what they believe are the requirements for their systems. Once the developers have interpreted what 'characteristics' their system will implement based on a FIPP, it allows them to proceed to develop a risk framework for their system to mitigate and control and underlying issues.

3.2 NIST Privacy Framework

Another approach to defining a framework for Information Technology systems involving an individual's personal information was published by the National Institute of Standards and Technology (NIST) in the United States. NIST Privacy Framework differs in approach from FIPPs. Instead of providing a high-level expectation at the

system level, the NIST Framework aims to define risk categories related to an organisation use of personal data.

The NIST framework also differs in that it is a voluntary framework, with the primary aim of assisting organisations to organise their privacy risks in order to determine, build, and evaluate their privacy governance programs.

3.3 ISO/IEC 27701:2019

Within the ISO27XXX series of certifications for organisations, related to Information Security Management Systems (ISMS), a privacy extension was created to establish, maintain, and improve Privacy Information Management Systems (PIMS). The standard provides a framework for organisations to manage privacy controls to reduce any risk to an individual's rights to privacy. ISO27701 has three main defining characteristics:

1. Compliance to Privacy Requirements;
2. Maintaining to demonstrate compliance to applicable privacy requirements to regulators;
3. ISO Certification to a standard which demonstrates and communicates compliance to privacy.

3.4 OECD Guidelines

Historically, the first real guidelines on Privacy in Information Technology arose from the Organisation for Economic Co-operation and Development's (OECD) guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines aim to provide basic rules to govern any transborder flows of personal data, in order to protect the information itself, and the privacy rights of an individual. The additional

benefit of these guidelines was that this was the first real attempt to provide a harmonisation between the different data protection laws and regulations in individual countries. The OECD developed the guidelines themselves with cooperation between European Councils and member states. With this in mind, the guidelines themselves are not legally binding but serve a purpose to provide a basis for regulation for countries with no privacy regulations, or to enhance countries with existing privacy laws.

As the OECD guidelines are not legally binding or tied to a specific geographical area, the guidelines allow for countries to sign up to these guidelines voluntarily. The aim of the principles is similar to the founding goals of the European Union, to be able to travel and trade between borders with no interference. Only in this sense, it covers the transmission of data between borders uninterrupted. In comparison to frameworks proposed in the United States, the OECD guidelines are not specific to a sector, public or private, or a specific industry. It also makes no distinction between whether data is collected electronically or by traditional methods.

The eight principles of the OECD guidelines are also comparable to the principles set out in GDPR, as shown below in table 2:

OEDC Guidelines	**GDPR Principles**
Collection Limitation Principle	Data Minimisation
Data Quality Principle	Accuracy
Purpose Specification Principle	Purpose Limitation
Use Limitation Principle	Storage Limitation
Security Safeguards Principle	Integrity and Confidentiality
Openness Principle	Lawfulness, Fairness, and Transparency
Individual Participation Principle	Data Subject Rights
Accountability Principle	Accountability

TABLE 2 - OECD AND GDPR COMPARISON

In chapter 5, a comparison of these principles and guidelines and how they can be translated into meaningful descriptions in order to be used by both legal and information technology professionals for assessing processing activities.

The main benefit to having a defined set of principles such as the ones above is that it allows for both the privacy professionals and information technology professionals to have a starting point on how to address the issue of compliance. While legal professionals have the necessary background to determine what regulation might or might not require a business to do. It is also essential to take into account the knowledge of information technology professionals to determine how to achieve what is required by the regulation. There may need to be further analysed to determine whether certain activities are even possible within the organisations current systems, and therefore allow the legal teams to prepare to make any exceptions to the rules that may need addressing.

5. PRIVACY REGULATIONS

4.1 General Data Protection Regulation

The General Data Protection Regulation as implemented by the European Commission is a method of legitimising the fundamental right to privacy of all European citizens as technology continues to progress at a pace which existing regulation cannot maintain. The General Data Protection Regulation governs rights and freedoms of individuals. For organisations, the regulation simplifies rules for businesses operating within the European Union; the regulation is not limited to organisations with headquarters located in EU; also, organisations which are 'founded' in a territory of the European Union are required to comply with the regulation.

Content-wise, the GDPR follows many concepts and principles as set out in its predecessor, the Data Protection Directive. However, the key difference relates to the Directive providing guidelines which are left open to interpretation in member states on how to implement their regulations based on this Directive. In contrast, the regulation builds further upon these and sets out several obligations and further details on how each article of the regulation should be interpreted.

For organisations operating within the European Union or processing the personal data of individuals who reside within the Union, the GDPR will affect the organisations in several ways:

- The GDPR applies to all member states within the European Union;
- GDPR is appliable to all organisations which process the personal data of European citizens;
- GDPR is appliable to all organisations processing personal data no matter whether that have determined if they are a Data Controller or a Data Processor;

- GDPR will be applicable to all organisations outside the European Union where a business offers goods or services or monitors the behaviour of citizens within the European Union;
- Individuals are in control of their personal data if an organisation relies on the consent mechanism for the processing of personal data, then consent but provided by an individual. By this, it means that an individual must not feel forced into a position in which they feel they have to give consent against their will in order to receive a service. Additionally, consent must be able to be withdrawn as freely as provided to an organisation.
- Organisations are required to be transparent with data processing activities ahead of any processing of personal data, or within a reasonable period after processing has already been initiated. Transparency also brings with it the requirement that it must be able to be read and fully understood by the target audience, for example, a privacy notice for children is required to be written in more simple terms a child could understand.
- With the enhancement of rights to individuals, organisations must also take into account. These rights sometimes referred to as "Subject Access Rights", including the rights to rectification, erasure, portability, and objection to the processing of personal data.
- For multinational organisations, the regulation provides new ways to legitimise any transfers of personal data outside of the European Union. Transfers are no longer limited to assessing the security safeguards in place from both parties, but now enables the option of allowing for Binding Corporate Rules or Standard contractual Clauses to legitimise the transfer of data. (European Parliament, 2016)

4.2 Privacy Laws of the United States

Within the United States, there is currently no one single comprehensive law which governs an individual right to privacy. Although this is the case, there are several constitutional limits on the level of intrusion into an individual's right to privacy (Philadelphia Convention, 1787).

The Fourth Amendment of the Constitution states that *"the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."* (Philadelphia Convention, 1787)

At present, the state of California is the only state which has enacted Privacy act designed to give its citizens similar rights to those with other national or regional laws, this is explained further in the next chapter.

In addition to the Constitution, many states have amendments or separate constitutions to provide the right to privacy of their citizens, as shown in the table below:

Alaska	The right of the people to privacy is recognised and shall not be infringed. The legislature shall implement this Section. (State of Alaska, 1956)
Arizona	No person shall be disturbed in his private affairs, or his home invaded, without the authority of law. (State of Arizona, n.d)
California	All people are, by nature, free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. (State of California, 1974)

Florida	Right to Privacy: Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This Section shall not be construed to limit the public's right of access to public records and meetings as provided by law. (The Florida Senate, 1980) Searches and Seizures - The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated. (The Florida Senate, 1980)
Hawaii	Section 6: Right to Privacy: The right of the people to privacy is recognised and shall not be infringed without the showing of compelling state interest. The legislature shall take affirmative steps to implement this right. (State of Hawaii, 1978) Section 7: Searches, Seizures and Invasion of Privacy The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and invasions of privacy shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized or the communications sought to be intercepted. (State of Hawaii, 1978)
Illinois	Section 6. Searches, Seizures, Privacy and Interceptions The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized. (State of Illinois, n.d)

Louisiana	Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. *No* warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search. Any person adversely affected by a search or seizure conducted in violation of this Section shall have the standing to raise its illegality in the appropriate court. (State of Louisiana, n.d)
Montana	The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of compelling state interest. (State of Montana, 1974)
New Hampshire	Right to Privacy. An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent. (State Constitution - Bill of Rights | NH.gov, 2018)
South Carolina	The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures *a*nd unreasonable invasions of privacy shall not be violated, and no Warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained. (State of South Carolina, n.d)
Washington	Invasion of Private Affairs or Home Prohibited No person shall be disturbed in his private affairs, or his home invaded, without the authority of law. (State of Washington, n.d)

4.3 California Consumer Privacy Act

The California Consumer Privacy Act (CCPA), which was passed into law in June 2018 to enhance the privacy rights specifically of the residents of California, United States, and came into enforcement in January 2020.

In comparison to the GDPR in the European Union, there are several 'intentions' which are similar to the 'principles laid out in GDPR. For organisations, these similarities apply:

- The California Consumer Protection Act requires organisations to be transparent with the personal data collected regarding citizens of the state of California.
- The requirements described in the act provides citizens of California with a mechanism to request an organisation provides information regarding what information is processed, any potential recipients to which data is sold or disclosed, and allows individuals access to personal information.
- Similar to GDPR, CCPA requires an organisation to be able to delete any personal information related to an individual upon request, and the opt-out mechanism of consent applies that an individual can opt-out from having their personal information sold to a third party.

In terms of applicability, there are some differences for organisations. CCPA applies to an organisation when one of the three criteria occur:

- The organisation has a gross annual revenue of more than $25 million;
- If the organisation purchases, receives or sells the personal information of over 50,000 individuals;
- An organisation receives more than half of its annual revenue from the sale of personal information.

4.4 Brazilian General Data Protection Act

In August 2018 Brazil published their first comprehensive privacy regulation, Lei Geral de Proteção de Dados (LGPD) or translated as Brazilian General Data Protection Act. The LGPD is aligned mainly to the European Union's GDPR.

The same terms of applicability apply with the LGPD, all organisations operating within Brazil or process the personal data of Brazilian citizens are subject to the regulation.

One critical addition to this regulation is there is an extra data subject right, that organisations but inform individuals of any personal data which has is shared with other public or private authorities.

In terms of lawful processing of personal information, the one key difference is the addition of processing of personal data in order to protect the credit score of the data controller.

6. PRIVACY PRINCIPLES AND FRAMEWORK CREATION

This chapter aims to attempt to find the middle ground between the requirements of privacy regulations to an organisation from both the legal perspective and that of an information technology perspective.

As we have seen in the previous chapters, there are several suggestions of a privacy framework which organisations should follow from an information technology perspective. In contrast, we have analysed the varied requirements or approaches that an organisation is obligated to adhere to from a legal perspective.

5.1 Scope

To further analyse the legal requirements into a list of development points for guidelines appropriate for information technology professionals, the first step is to set the scope limitations for this analysis.

In terms of geographical coverage, the European Union's General Data Protection Regulation will be at the forefront of this analysis, for example, the Brazilian General Data Protection Act, and the Californian Consumer Protection Act both adopt the main principles of GDPR for their regulations. While there are additional upcoming regulations, such as Illinois' Data Transparency and Privacy Act and the Indian Personal Data Protection Bill, for this analysis, I will predominantly assess GDPR and CCPA as the primary regulations.

With Information Technology governance, there are many frameworks which attempt to cover all elements of what it termed as Governance, Risk, and Compliance, or GRC. These frameworks all offer a different perspective on how the overarching governance of information technology systems. For this analysis, in order to build privacy

guidelines for information technology professionals to understand, I believe it is essential to use an industry-standard or best practice methodology. I believe this would be the best approach as in larger multinational organisations, and many information technology teams would most likely have experience in meeting industry best practices for audits or certifications, such as the ISO27XXX series.

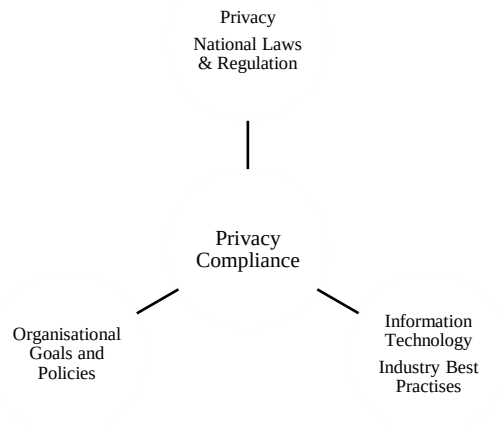
5.2 Governance Framework

For stakeholders to understand the role privacy will play in an organisation, it is essential to breakdown each element of the legal requirements into elements to communicate why their role in achieving compliance to a legal regulation is necessary and what their part to play is.

For this analysis, the topics for analysis will be the following:

7. Privacy Regulation Requirements
8. Organisational Privacy Policy and Notices
9. Organisational Internal Controls
10. Organisational Security Controls
11. Industry Standard Privacy and Security Controls

The three major critical components of creating a privacy compliance program arise from laws and regulation, organisational goals and policies, and information technology industry best practices, as shown in the following diagram, these three flows into attempting to achieve privacy compliance.



5.2.1 Assumptions

For further analysis and creation of a Privacy Framework within an organisation, the analysis will be based on the following assumptions for an organisation. These assumptions have been chosen to allow for a broader perspective for an organisation that may cover one of more legislative jurisdictions.

- The organisation will have a global revenue of more than $25 million;
- The organisation will operate on a global scale;
- The organisation will have a legal function;
- The organisation will have an information technology governance function;
- The organisation will have an information technology operations function.

5.2.2 Privacy Regulation Requirements

Privacy regulations and seeking to reduce brande damage are the key drivers behind an organisation decision for creating a privacy governance program. The process of determining the privacy regulations which are relevant to an organisation is divided into the following steps:

Step One – Geographical Scope

For an organisation to start to achieve compliance, they must first take a look at the countries in which they are physically located and where their consumer base is.

Step Two – Regulation Applicability

Once the scope is narrowed down to a geographical area of applicability, the next stage is to determine which regulations apply to an organisation. California's CCPA is only appliable to organisations with revenue over $25 million, or where the sale of personal information generates their primary source of revenue. Whereas, regulations such as GDPR applies to any organisation processing personal information of its citizens, the same for Brazil's LGDP.

Step Three – Regulation Comparison

In the final stage of this evaluation is to find similarities between regulations. By finding similarities, this will aid in the creation of organisation-wide policies. For this thesis, the scope is narrowed to countries with stricter regulations. Table 3 provides an example as set out in Article 6 (Legal Bases) of the European Union’s GDPR as the primary regulation to be compared to, as it is currently the most comprehensive of regulations.

General Data Protection Regulation (European Parliament, 2016)	**Brazilian General Data Protection Act** (Brazilian Data Protection Law (LGPD, English translation), 2018)	**India Personal Data Protection Bill** (Sabha, L., & Republic of India, 2019)	**California Consumer Privacy Act**
Article 6	Article 7	Chapter II and III	No Provisions
Consent	Consent	Consent	
Performance of a contract	Performance of a contract		
Legal obligation(s)	Legal or regulatory obligation(s)	Legal Obligation(s)	
Protection and Vital Interests	Protection of life or physical safety	Medical Emergencies related to a threat to life	
Public Interest	Public Administration or Interest		
Legitimate interests	Legitimate interests	Reasonable Purposes *(restriction of purposes or interests)*	

	Research purposes		
	Judicial, administrative or arbitration procedures		
	Related to a procedure carried out by health professionals, health services or sanitary authorities;	Provision of medical treatment or health services	
	Protection of credit,		
		Employment Purposes	

TABLE 3 - COMPARISON OF LEGAL BASES

As shown in the example related to Article 6 of the General Data Protection Regulation in table 3, we can see that from a comparison of three other current privacy regulations there are some overlaps in requirements, such as obtaining consent before processing, and most commonly that there must be a legal reason for processing to occur.

The significant outlier in this analysis is that the California Consumer Protection Act provides no requirements regarding the legal bases for processing personal data.

The next comparison to demonstrate this will be related to Chapter 3 of the General Data Protection Act, which provides the requirements to organisations regarding the rights of a data subject.

General Data Protection Regulation (European Parliament, 2016)	**Brazilian General Data Protection Act** (Brazilian Data Protection Law (LGPD, English translation), 2018) (What is the LGPD? Brazil's version of the GDPR - . , 2020)	**India** **Personal Data Protection Bill** (Sabha, L., & Republic of India, 2019)	**California Consumer Privacy Act** (State of California, 2018)
Chapter 3	Article 18	Chapter V	1798.XXX
Right of Access	Right to Confirmation Right to Access	Right to Confirmation and Access	Right to Access
Right to Rectification	Right to Correction	Right to Correction and Erasure	
Right to Erasure	Right to erasure (based on consent)		Right to erasure
Right to Restriction		Right to be forgotten	Right to opt-out
Right to Data Portability	Right to Data Portability	Right to Data Portability	Right to portability
Right to Object	Right to information about the possibility of denying consent and the consequences of such denial		
	Right to information about public and private entities with which the controller has shared data		Right to be informed.

TABLE 4 - DATA SUBJECT RIGHTS

Table 4 shows that there are more similarities with existing regulations in terms of the rights that individuals or data subjects have in terms of what they can expect of companies that are processing their personal information.

Whereas Table 3 shows that while there are some countries which provide more comprehensive regulations regarding allowing organisations to process an individual's personal data.

5.2.3 Organisational Compliance Requirements

Regarding creating an organisational policy to provide guidance on when it is allowed or appropriate to process personal data, policymakers must take into account their organisations operating model, whether there are multiple operating companies within an organisation which create and maintain their policies at a country or regional level, or whether the organisation is in a position where the global policy would be more appropriate to set a standard for any activities which may process personal data.

To create policies based on the findings in Table 3 an organisation would need to determine which is more appropriate, to create policies which are relevant on a local scale or to create an overarching global policy to govern how an organisation as a whole will operate with an individual's personal data. As the California Consumer Protection Act does not provide guidelines on the collection of personal data, an organisation could decide to follow one of the following scenarios:

- Localised Policy – As there are no restrictions on the collection of personal information, a localised policy would not be required to mention any guidelines on how an Information Technology team should realise a new system or processing activity.

- Global Policy (Risk-Based) – An organisation could use the analysis provide in table 3 to determine which are the most common attributes of privacy regulations and enforce a policy which would only cover the most common risks. From Table 3, the observation that Consent, Legal Obligations, Medical Emergencies, and Legitimate Interests are the most common legal bases for collection. Therefore, a policy must be explicitly created regarding these.

  This approach is applied to the findings in Table 4, where we can see that for the majority of regulatory requirements, there is a significant overlap in what rights an individual can expect concerning their personal information.

- Global Policy (Enforcement Based) – Another approach an organisation could undertake would be to assess the potential enforcement actions that can be taken against an organisation should they not be compliant with the law. As the Brazilian Data General Protection Act does not specify any penalties for non-compliance, the risk associated would only correspond to a loss of trust or reputation to an organisation. Whereas both the General Data Protection Regulation and the California Consumer Protection Act both specify penalties which will result should an organisation be non-compliant with regulations.

- Global Policy (Local Amendments) – Similar to the risk-based approach for global policy, one alternative could be to create a global policy which covers all the most common regulatory requirements. In Table 4, we see that the Right to Access is present in all four regulations. However, the 'Right to information about the possibility of denying consent and the consequences of such denial' is only present in the Brazilian regulation. Therefore, an organisation could opt to create a specific amendment to its policy for Brazil.

The risk associated with this is that although the approach would allow for all requirements of country-specific regulations to be covered, it creates a splintering effect for an organisation to implement. A Data Subject Access Rights process, the process in which an individual can assert their rights concerning their personal information, such as the right to erasure, would then require separate policies and procedures per country or region. Therefore, creating complexity within the IT systems processing the requests, resources in terms of the costs associated with training employees to adapt to the specific requirements should a request come from an area with what can be very slight differences compared to other regulations. There is a significant effort a company requires to create and adapt their systems to comply with individual regulations. Table 4 - Data Subject

Ultimately the approach which an organisation wishes to take will depend on the size of an organisation, and the resources dedicated to fulfilling any governance and compliance activities. An organisation with dedicated resources to the required functions at a country or regional level can choose to go for the localised amendment approach. Whereas, even for a large organisation in the early phases of establishing privacy governance and compliance structure, a suggestion is that starting with the risk-based approach to build the foundations of privacy governance and then later maturing into the ability to cover all regulations is the best approach.

5.2.3.1 Adapting the regulatory requirements into policy

In order to create an organisation policy regarding the subject access rights, we can take the information collected in Table 4, and analyse the regulatory requirements to create

an organisational requirement. For this, the Rights of Data Portability, Erasure, and Rectification will be specifically analysed.

Right to Data Portability	
GDPR	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and **machine-readable format** and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided … (European Parliament, 2016)
LGPD	The data subject … has the right to obtain the following from the controller: V – portability of the **data** to another service provider or product provider … (Pereira Neto Macedo Advogados, 2018)
PDPB	… the data principal shall have the right to— (a) receive … **personal data** in a structured, commonly used and **machine-readable format** (Sabha, L., & Republic of India, 2019)
CCPA	No equivalent right(s)

Potential Organisational Compliance Requirement:

Personal information must be available in a machine-readable format

Right to Erasure	
GDPR	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have an obligation to **erase personal data** without undue delay … (European Parliament, 2016)
LGPD	The data subject … has the right to obtain the following from the controller: VI – **deletion** of personal data processed with the consent of the **data subject** … (Pereira Neto Macedo Advogados, 2018)
PDPB	The data principal shall where necessary … have the right to— … (d) the **erasure** of **personal data** which is no longer necessary for the **purpose** for which it was processed. (Sabha, L., & Republic of India, 2019)
CCPA	A consumer shall have the right to request that a business **delete** any personal information about the **consumer** which the business has collected from the consumer. (State of California, 2018)

Potential Organisational Compliance Requirement:

Personal information must be erasable upon request of an individual, where applicable by law and is no longer required for the intended purposes.

Right to Rectification	
GDPR	The **data subject** shall have the right to obtain from the controller without undue delay the **rectification** of inaccurate **personal data** concerning him or her. (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016)
LGPD	The **data subject** … has the right to obtain the following from the controller: III – **correction** of incomplete, inaccurate or out-of-date data; (Pereira Neto Macedo Advogados, 2018)
PDPB	The **data principal** shall where necessary … have the right to— (a) the **correction** of inaccurate or misleading personal data; (b) the completion of incomplete personal data; (c) the **updating** of **personal data** that is out-of-date; … (Sabha, L., & Republic of India, 2019)
CCPA	No equivalent right(s)

Potential Organisational Compliance Requirement:

Any personal information must be rectifiable upon request of an individual, where applicable by law.

5.2.4 Industry Standard Privacy and Security Controls

Information Technology is a crucial element of any privacy governance or compliance program in an organisation. Technology is both one of the main challenges of a privacy program, as technology evolves, so does the need to implement adequate measures to protect the privacy of individuals. At the same time, information technology is also an opportunity for privacy programs to build upon to mature.

Information Management Systems are continually developing to both aid and embed the need for privacy-by-design and privacy by default. Most major Information Security Governance, Risk, and Compliance tools now include pre-designed assessment, risk analysis, risk mitigation, and data discovery abilities which benefit a privacy program.

Within an organisation, the Information Security teams play a role in assisting both the organisations' Information Technology and other external regulatory compliance activities, such as PCI, SOX, ISO27XXX, and ISO9XXX compliance. As mentioned at the start of this chapter, the primary goal is to find the middle ground between regulatory requirements, and the understanding of how Information Technology professionals can understand expectation in order to achieve compliance. As privacy regulations are somewhat abstract and difficult to comprehend fully, the ability that information security or privacy professionals have to translate regulations into understandable terminology is a determining factor to whether a privacy compliance program will function and continue to mature. In most large organisations, the Information Security departments will use a combination of internal standards and controls based upon industry best practices and frameworks, such as ISO, NIST, and COBIT. These frameworks and standards are based upon years of standardisation and

maturity to be able to provide all organisations with a baseline for expectations from an organisation.

For Privacy in Information Technology teams, two recent frameworks have tried to address the gaps in understanding the requirements of privacy regulations.

- The NIST Privacy Framework (January 2020)
- ISO27701:2019 Privacy Information Management (August 2019)

While both these frameworks provide guidelines to Information Technology professionals on meaningful standards and controls to implement, there is still the middle ground on demonstrating to stakeholders and the organisation that these controls meet the requirements of privacy regulation.

An example of this could be related to CT.DM-P6 of the NIST Privacy Framework, which states that "Data are transmitted using a standardised format" (National Institute of Standards and Technology, 2020). To a Legal Professional, with no context this would just appear to be a control that requires all data to be transmitted in a particular format, not specifying the purpose behind it. To an Information Technology professional, this will appear as a control that they need to develop their systems with a standardised data architecture in place, such as XML. However, likewise, to the Legal Professional, there is no context behind why this needs to occur.

In order to adapt existing privacy or information security framework into useable guidelines for Information Technology professionals to use, the guidelines must be presented in comprehendible terms to demonstrate how the controls will assist with achieving privacy compliance in an organisation. The next stage is for stakeholders from both Information Technology, Legal, and Privacy departments to analyse the

controls provided by the frameworks and compare these to the requirements from regulations.

For this analysis, the previous information analysed to create a corporate compliance requirement will be assessed to see which of the controls from the NIST Privacy Framework apply or are best suited to meet the regulatory requirement.

Right to Data Portability	
GDPR	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided … (European Parliament, 2016)
LGPD	The data subject … has the right to obtain the following from the controller: V – portability of the data to another service provider or product provider … (Pereira Neto Macedo Advogados, 2018)
PDPB	… the data principal shall have the right to— (a) receive … personal data in a structured, commonly used and machine-readable format (Sabha, L., & Republic of India, 2019)
CCPA	No equivalent right(s)
Organisational Compliance Requirement	Personal information must be available in a machine-readable format.

Potential Industry Standard Controls for Privacy:

CT.PO-P2: Policies, processes, and procedures for enabling data review, **transfer, sharing or disclosure**, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).

CT.PO-P3: Policies, processes, and procedures for enabling **individuals' data processing** preferences and **requests** are established and in place

CT.DM-P6: Data is transmitted using **a standardised format**

Right to Erasure	
GDPR	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have an obligation to erase personal data without undue delay … (European Parliament, 2016)
LGPD	The data subject … has the right to obtain the following from the controller: VI – deletion of personal data processed with the consent of the data subject … (Pereira Neto Macedo Advogados, 2018)
PDPB	The data principal shall where necessary … have the right to— … (d) the erasure of personal data which is no longer necessary for the purpose for which it was processed. (Sabha, L., & Republic of India, 2019)
CCPA	A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (State of California, 2018)
Organisational Compliance Requirement	Personal information must be erasable upon request of an individual, where applicable by law and is no longer required for the intended purposes.

Potential Industry Standard Controls for Privacy:

CT.PO-P1: Policies, processes, and procedures for authorising data processing (e.g., organisational decisions, **individual consent**), **revoking authorisations**, and maintaining authorisations are established and in place

CM.AW-P5: **Data** corrections or **deletions** can be communicated to individuals or organisations (e.g., data sources) in the data processing ecosystem.

CT.DM-P4: Data elements can be accessed for **deletion**.

CT.DM-P5: Data is **destroyed** according to policy

Right to Rectification	
GDPR	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016)
LGPD	The data subject … has the right to obtain the following from the controller: III – correction of incomplete, inaccurate or out-of-date data; (Pereira Neto Macedo Advogados, 2018)
PDPB	The data principal shall where necessary … have the right to— (a) the correction of inaccurate or misleading personal data; (b) the completion of incomplete personal data; (c) the updating of personal data that is out-of-date; … (Sabha, L., & Republic of India, 2019)
CCPA	No equivalent right(s)
Organisational Compliance Requirement	Any personal information must be rectifiable upon request of an individual, where applicable by law.

Potential Industry Standard Controls for Privacy:

CT.PO-P2: Policies, processes, and procedures for enabling **data** review, transfer, sharing or disclosure, **alteration**, and deletion are established and in place (e.g., to maintain **data quality**, manage data retention).

CT.PO-P3: Policies, processes, and procedures for enabling **individuals' data** processing preferences and **requests** are established and in place

CM.AW-P5: **Data corrections** or deletions can be communicated to individuals or organisations (e.g., data sources) in the data processing ecosystem.

CT.DM-P3: Data elements can be accessed for **alteration**.

Information Technology Requirement Statements

The final stage of preparing a framework is to combine the regulation, organisational, and industry best practice requirements into a set of statements to define how privacy and information technology combined will help achieve compliance to any in-scope regulations.

In this final stage of analysis, requirement statements are constructed to guide stakeholders, and the following requirements will apply:

- A reference to individuals or data subjects;
- A reference to the applicable law;
- And a reference to the expectation of information technology.

With these three elements in each statement, the statements should be able to cover the grey area that lies between regulatory requirements, and the requirements of information technology, and provide an overview of how compliance is achieved.

Right to Data Portability	
GDPR	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided … (European Parliament, 2016)
LGPD	The data subject … has the right to obtain the following from the controller: V – portability of the data to another service provider or product provider … (Pereira Neto Macedo Advogados, 2018)
PDPB	… the data principal shall have the right to— (a) receive … personal data in a structured, commonly used and machine-readable format (Sabha, L., & Republic of India, 2019)
CCPA	No equivalent right(s)
Organisational Compliance Requirement	Personal information must be available in a machine-readable format.
Industry Best Practices	CT.PO-P2: Policies, processes, and procedures for enabling data review, **transfer, sharing or disclosure**, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention). CT.PO-P3: Policies, processes, and procedures for enabling **individuals' data processing** preferences and **requests** are established and in place CT.DM-P6: Data is transmitted using **a standardised format**

Potential Information Technology Requirement Statement:

Applications and systems must implement the functionality to export an individual's data upon request in machine-readable format to satisfy data subject access requests.

Right to Erasure	
GDPR	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have an obligation to erase personal data without undue delay … (European Parliament, 2016)
LGPD	The data subject … has the right to obtain the following from the controller: VI – deletion of personal data processed with the consent of the data subject … (Pereira Neto Macedo Advogados, 2018)
PDPB	The data principal shall where necessary … have the right to— … (d) the erasure of personal data which is no longer necessary for the purpose for which it was processed. (Sabha, L., & Republic of India, 2019)
CCPA	A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (State of California, 2018)
Organisational Compliance Requirement	Personal information must be erasable upon request of an individual, where applicable by law and is no longer required for the intended purposes.
Industry Best Practices	CT.PO-P1: Policies, processes, and procedures for authorising data processing (e.g., organisational decisions, **individual consent**), **revoking authorisations**, and maintaining authorisations are established and in place CM.AW-P5: **Data** corrections or **deletions** can be communicated to individuals or organisations (e.g., data sources) in the data processing ecosystem. CT.DM-P4: Data elements can be accessed for **deletion**. CT.DM-P5: Data is **destroyed** according to policy

Potential Information Technology Requirement Statements

Applications and systems must implement the functionality to erase or restrict an individual's data upon request to satisfy data subject access requests.

Right to Rectification	
GDPR	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016)
LGPD	The data subject … has the right to obtain the following from the controller: III – correction of incomplete, inaccurate or out-of-date data; (Pereira Neto Macedo Advogados, 2018)
PDPB	The data principal shall where necessary … have the right to— (a) the correction of inaccurate or misleading personal data; (b) the completion of incomplete personal data; (c) the updating of personal data that is out-of-date; … (Sabha, L., & Republic of India, 2019)
CCPA	No equivalent right(s)
Organisational Compliance Requirement	Any personal information must be rectifiable upon request of an individual, where applicable by law.
Industry Best Practices	CT.PO-P2: Policies, processes, and procedures for enabling **data** review, transfer, sharing or disclosure, **alteration**, and deletion are established and in place (e.g., to maintain **data quality**, manage data retention). CT.PO-P3: Policies, processes, and procedures for enabling **individuals' data** processing preferences and **requests** are established and in place CM.AW-P5: **Data corrections** or deletions can be communicated to individuals or organisations (e.g., data sources) in the data processing ecosystem. CT.DM-P3: Data elements can be accessed for **alteration**.

Potential Information Technology Requirement Statements

Applications and systems must implement the functionality to amend an individual's data upon request to satisfy data subject access requests.

6. IMPLEMENTATION OF A PRIVACY RISK FRAMEWORK

For this chapter a further step shall now be undertaken in order to show how the analysis of chapter 5 will work in practice.

In the previous chapters a complete overview of the theory behind the creation and evaluation methodology for an Information Systems Framework has been reviewed, and examples of Privacy legislations and existing frameworks have been analysed.

As part of its business operations, an organisation will often need to process personal data. This personal data is any information relating to an identified or identifiable natural person. An identifiable natural person is someone who can be identified directly or indirectly by reference to an identifier, such as name, address, e-mail address, cookie ID, IP address or location data. Further to this the term "processing" means any operation performed on Personal Data, such as access, view, use, transfer, share, collect, store, alter, disclose, restrict and erase.

For the purpose of this implementation we will limit our scope to Europe as the predominant area of relevance. Therefore, any processing of Personal Data is subject to the requirements following from the General Data Protection Regulation and any applicable local Personal Data protection laws and regulations.

In order to ensure that a processing activity complies with the GDPR, each processing activity will be subject to a privacy risk evaluation.

From my own working experiences in the field of privacy within a multinational organisation, as part of ensuring a processing activity is compliant with GDPR the general expectation from a stakeholder within the organisation is the expectation that a privacy practitioner should "make it GDPR compliant". This ask is, from experience,

significantly more difficult than it sounds from just one sentence. Ensuring a processing activity is compliant to GDPR a process known as a Data Protection Impact Assessment takes place, these assessments are designed to assessed the intentions of a processing activity and any associated risks involved. In order to demonstrate this further, table 5 expands upon the fundamental privacy compliance activities placed upon an organisation from GDPR and any additional requirements from an organisation.

PRIVACY COMPLIANCE FUNDAMENTALS	EXPLANATION
1. Transparency	Individuals must be informed how their personal data is processed. This is typically achieved through a privacy notice.
2. Legal Ground & Specific Purpose	One of six legal grounds for processing personal data must apply to the processing activity. Personal data must be processed for a specific purpose.
3. Legal Ground (special categories of personal data).	In the event special categories of personal data are processed, one of the legal bases applicable to processing special categories of personal data must apply.
4.Data Minimization	Personal data as part of a processing activity must be adequate, relevant and limited to what is needed for the purpose it is processed.
5. Data Quality	Personal data must be kept up to date and accurate.

6.Data Retention	Personal data must not be retained longer than necessary and erased once the processing of personal data is no longer necessary for the purpose it is processed.
7.Data Subject Rights	Where relevant, a processing activity must allow for the exercise of data subject rights, e.g. erasure of personal data, access to personal data, objection to the processing of personal data.
8. International Transfers	In the event personal data related to EEA citizens is transferred outside the EEA, this transfer must be legitimized by Binding Corporate Rules, or Model Contract Clauses for transfers of personal data to third parties.
9.Third Parties	In the event a third party has access to personal data in any form (storage, access, viewing on a computer screen), specific data protection clauses need to be included in the contract with the third party. Access to personal data must be limited.
10. Reporting	Internal stakeholders that can access personal data must be limited. Onward processing of personal data (through API's, etc.) must be compliant with an organisations privacy policy.
11. Security	Any processing activity must have ensured that the appropriate security safeguards are in place to ensure the integrity of personal data.
12. Access	Access to personal data must be limited to those individuals that have a legitimate need to view the personal data.
13.Works Council	In European organisations the processing of personal data related to employees may be subject to works council consultation or consent.

Further expansion on these fundamentals will be required to make these into useable controls for an organisation. To start this process, I will first expand upon each fundamental by conducting with fellow privacy practitioners, from both a legal and an IT compliance background.

In these interviews I hope to gain an understanding of the experiences from practitioners within the same organisation when conducting an assessment and relating these findings back to each fundamental in the form of a decision tree. These interviews will be conducted by video call on a one-on-one basis, to try and limit any influence on the responses provided from different job levels and backgrounds. Each of these interviews was scheduled for a period of 30 minutes, with an additional 15 minutes allowed for any additional clarifications.

As a result of these interviews I have managed to gather information in regard to how fellow privacy practitioners interacted with a variety of different stakeholders within an organisation.

In order to create a 'Business Requirement' for each of the following privacy fundamentals, the following logic was applied, and then re-evaluated with the interviewee:

1. Discover what would be required for a processing activity to be compliant;
2. Discover what would be required for a processing activity to not be compliant;
3. Determine what the business/procedural requirement would be for compliance;

The questions asked during these interviews are as follows:

Category	Question(s)

Compliance	• For this 'Privacy Fundamental' please describe instances of how a processing activity would demonstrate it is compliant • For this 'Privacy Fundamental' please describe instances of how a processing activity would demonstrate it is non-compliant • For this 'Privacy Fundamental' please describe instances of how a processing activity lies between compliance and non-compliance
Composability	• For this 'Privacy Fundamental' to what extent would a business benefit from aligning privacy controls/requirements with an existing framework? • For this 'Privacy Fundamental' to what extent would a business not benefit from aligning privacy controls/requirements with an existing framework?
Reusability	• For this 'Privacy Fundamental' to what extent would a business benefit from having standardised controls/requirements? • For this 'Privacy Fundamental' to what extent would a business not benefit from having standardised controls/requirements? • For this 'Privacy Fundamental' are there any limitations which would prevent reusable/repeatable controls?
Maintainability	• For this 'Privacy Fundamental' to what extent does a 'current control' require adaptation for a specific processing activity? • For this 'Privacy Fundamental' to what extent would a business benefit from a generalised control which can be used to provide high level guidance?

For the evaluation aspect of this chapter, the primary focus will be on the following methods as stated previously in Chapter 2, with the following questions:

Category	Questions
Standardisation	• To what degree does the format of the proposed Privacy Fundamental effectively communicate the requirements? • To what degree does the content of the proposed Privacy Fundamental provide adequate information regarding requirements?
Abstraction	• To what degree can the proposed Privacy Fundamental be published to provide only the base line requirements expected from the stakeholders? • To what degree do you agree that the proposed Privacy Fundamental provides enough information for stakeholders to implement requirements?
Loose Coupling	• To what degree is the proposed Privacy Fundamental structured to act independently from other Privacy Fundamentals or requirements?
Autonomy	• To what degree to you agree that significant change to the proposed Privacy Fundamental would affect other Privacy Fundamentals as a result?
Genericity	• To what degree do you agree that the format of the proposed Privacy Fundamental can be reused?

	• To what degree do you agree that the requirements of the proposed Privacy Fundamental can be reused in additional Fundamentals?
Discoverability	• To what degree do you agree that related Privacy Fundamentals should be referenced in the content of this proposed Privacy Fundamental? • To what degree that the referenced GDPR Requirements should be made available as part of the proposed Privacy Fundamental? • To what degree that the referenced NIST Controls should be made available as part of the proposed Privacy Fundamental?
Composability	• To what degree to you agree that new Privacy Fundamentals could be drafted as a result of this proposed Privacy Fundamental? • To what degree to you agree this Privacy Fundamentals could be merged with another Privacy Fundamental?

A further expansion on each Privacy Compliance Domain is provided in Appendix 1.

The results of the interviews conducted are shown in the table in Appendix 2.

6.1 Transparency

This fundamental principle requires that an organisation is transparent with individuals as to the processing of their personal data. In order to comply with the transparency requirement of the GDPR, a privacy notice is typically provided to an individual. In

practice, whether and how a privacy notice is provided will depend on the type of individuals and the personal data processed.

6.1.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.1.1*
Composability	The feedback for this interview category was: • There would be no perceived benefit of directly linking to an existing framework from a legal perspective; • The would be a benefit from an IT perspective to embed the transparency requirement into the design process
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding transparency; • The Business would require resources to ensure employees were aware of whether an activity falls within a particular notice
Maintainability	The feedback for this interview category was: • Currently the business is required to tailor each requirement based on the category of individual, and how notice is provided; • The Business would benefit from having predefined controls that can be reused to each situation

6.1.3 Proposed Business Requirements

- Control #1.1: the responsible ‘project manager’ must ensure that the project is in line with an existing privacy notice.

- Control #1.2: the responsible ‘project manager’ must ensure that a bespoke privacy notice is implemented.
- Control #1.3: the responsible ‘project manager’ must ensure the existing bespoke notice complies with applicable data protection laws.
- Control #1.4: the responsible ‘project manager’ must ensure that a copy of the existing bespoke privacy notice is provided to the privacy team.

6.1.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The Privacy Fundamental is structed to act as independent control if necessary;
    - The Privacy Fundamental would affect other controls should changes occur;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;
    - The Privacy Fundamental should make available the text of NIST control requirements;

- Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
- The Privacy Fundamental could be merged with another Privacy Fundamental;

- On average those interviewed disagreed that:
  - The Privacy Fundamental contained adequate information regarding requirements;
  - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;

6.2 Legal Ground

The processing of Personal Data is only lawful if and to the extent that at least one of the following legal grounds applies:

1. The individual has given consent;

2. The processing is necessary for the performance of a contract;

3. The processing is necessary for compliance with a legal obligation;

4. The processing is necessary in order to protect the vital interests of the individual or another natural person.

5. The processing is necessary for the performance of a task carried out in the public interest or exercise of official authority vested.

6. The processing is necessary for the purposes of the legitimate interests pursued by an organisation or a third party.

6.2.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.2.1*
Composability	The feedback for this interview category was: • There would be a perceived benefit of directly linking to an existing framework by providing guidance on what is required for each legal ground;
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding legal grounds; • The Business would require resources to ensure employees were aware of whether an activity falls within a particular legal ground; • The Business may require significant modification to provide mechanisms to monitor consent in existing systems;
Maintainability	The feedback for this interview category was: • Currently the business is required to tailor each requirement based on the legal grounds for processing; • The Business would benefit from having predefined controls that can be reused to each situation

6.2.2 Proposed Business Requirements

- Control #2.1: The processing activity is covered by compliance with a legal obligation.

- Control #2.2: The processing activity is covered by legitimate interests. A Legitimate Interest Test must be completed and the organisations interests must be proportionate, clearly explained and necessary.
- Control #2.3: The processing activity is covered by the 'performance of a contract'' legal ground, evidence of the relevant contract must be provided.
- Control #2.4: The processing activity is covered by the 'consent' legal ground, the project manager of the processing activity must ensure consent is recorded / ensure consent can be revoked by an individual / provide evidence of consent.

6.2.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The Privacy Fundamental is structed to act as independent control if necessary;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;
    - The Privacy Fundamental should make available the text of NIST control requirements;

- Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
- The Privacy Fundamental could be merged with another Privacy Fundamental;

- On average those interviewed disagreed that:
  - The Privacy Fundamental contained adequate information regarding requirements;
  - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
  - The Privacy Fundamental would affect other controls should changes occur;

6.3 Legal Ground for Processing Special Categories of Personal Data

Special categories of personal data are types of personal data that are deemed to be particularly sensitive, which warrants additional protections from a data protection perspective. Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. As a general rule, organisations should avoid processing special categories of personal data where possible.

6.3.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.3.1*
Composability	The feedback for this interview category was:

	• There would be a perceived benefit of directly linking to an existing framework by providing guidance on what is required for each legal ground;
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding legal grounds; • The Business would require resources to ensure employees were aware of whether an activity falls within a particular legal ground; • The Business would require resources to ensure employees were aware of whether a data element is classified as a special category; • The Business would require resources to ensure employees were aware of the harms to an individual that may result in the processing of a particular special category
Maintainability	The feedback for this interview category was: • Currently the business is required to tailor each requirement based on the legal grounds for processing; • The Business would benefit from having predefined controls that can be reused to each situation

6.3.2 Proposed Business Requirements

- Control #3.1: The IT / Business Owner must obtain approval from the legal department prior to processing special categories of personal.6.3.4 Evaluation of Business Requirements

6.3.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The Privacy Fundamental is structed to act as independent control if necessary;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;
    - The Privacy Fundamental should make available the text of NIST control requirements;
    - The Privacy Fundamental could be merged with another Privacy Fundamental;
- On average those interviewed disagreed that:
    - The Privacy Fundamental contained adequate information regarding requirements;
    - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;

- The Privacy Fundamental would affect other controls should changes occur;
- Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;

6.4 Data Minimization & Purpose Limitation

Organisations are only allowed to process Personal Data that are adequate, relevant and strictly necessary for the purposes the organisation is processing the Personal Data for.

6.4.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.4.1*
Composability	The feedback for this interview category was: • There would be a perceived benefit of directly linking to an existing framework from a legal perspective by providing guidance why it is important to only process the data you really require; • The would be a benefit from an IT perspective to embed the data minimisation requirement into the design process
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding data minimisation; • The Business would require resources to increase awareness regarding data minimisation
Maintainability	The feedback for this interview category was:

	• Currently the business is required to manually review each processing activities data requirements then tailor each requirement based on the intended data elements for processing; • The Business would benefit from having predefined controls that can be reused to each situation, but would benefit more from a defined review methodology or framework.

6.4.2 Proposed Business Requirement

- Control #4.1 The project manager must justify the processing of such personal data elements by specifying why these data elements are strictly necessary for execution of the processing activity. If no justification is provided, the project cannot process such personal data elements

6.4.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;

  - The Privacy Fundamental should make available the text of GDPR requirements;
  - The Privacy Fundamental should make available the text of NIST control requirements;

- On average those interviewed disagreed that:
  - The Privacy Fundamental contained adequate information regarding requirements;
  - The Privacy Fundamental is structed to act as independent control if necessary;
  - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
  - The Privacy Fundamental would affect other controls should changes occur;
  - Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
  - The Privacy Fundamental could be merged with another Privacy Fundamental;

6.5 Data Accuracy

Personal data need to be accurate and kept up to date. Organisations must take reasonable steps to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

6.5.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.5.1*

Composability	The feedback for this interview category was: • There would be a perceived benefit of directly linking to an existing framework by providing guidance on what is required for ensuring data accuracy; • The would be a benefit from an IT perspective to embed the accuracy requirement into the design process • The would be a benefit from an IT perspective to embed the removal/suspension requirement into the design process
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding accuracy; • The Business may require significant modification to provide mechanisms to allow data to be updated/deleted in existing systems, and to ensure data updates are cascaded;
Maintainability	The feedback for this interview category was: • Currently the business provides three options for data accuracy; • It is unclear how this could be built further upon as a business requirement, but specific control lists could be provided and updated

6.5.2 Proposed Framework Control Description

- Control #5.1 The project manager must ensure capabilities to ensure the accuracy of personal data are implemented.

- Control #5.2 The project manager must ensure capabilities to remove personal data are implemented.

6.5.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental contained adequate information regarding requirements;
    - The Privacy Fundamental is structed to act as independent control if necessary;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;
    - The Privacy Fundamental should make available the text of NIST control requirements;
    - The Privacy Fundamental could be merged with another Privacy Fundamental;
    - The Privacy Fundamental would affect other controls should changes occur;
- On average those interviewed disagreed that:

- The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
- The Privacy Fundamental displays the baseline requirements for stakeholders;
- Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;

6.6 Retention

Organisations are only allowed to process Personal Data as long as necessary to serve the purpose of processing those Personal Data.

6.6.1 Interview Feedback

Category	Question(s)
Compliance	The feedback for this interview category was: • There would be a perceived no benefit of directly linking to an existing framework by providing guidance on what is required for ensuring data retention; • From a GDPR perspective, retention is specified only "processed as long as truly necessary", there are no specific legal guidelines • The would be a benefit from an IT perspective to embed the data retention requirement into the design process • The would be a benefit from an IT perspective to embed the data retention requirement into the design process
Composability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding data retention;

	• The Business may require significant resources to create and implement a data retention schedule;
Reusability	The feedback for this interview category was: • Currently the business provides two specific options for data retention; • It is unclear how this could be built further upon as a business requirement, but specific control lists could be provided and updated
Maintainability	The feedback for this interview category was: • The data retention fundamental controls could only be maintainable to the point where a data retention schedule was developed in order to reference retention times; • Ultimately it was discovered that amongst privacy practitioners, data retention is only a high-level concern, it should be placed with data governance

6.6.2 Proposed Business Requirement

- Risk #6.1: project manager must establish retention times for the personal data processed as part of the processing activity.

6.6.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:

- The format of the Privacy Fundaments effectively communicates the requirements;
- The Privacy Fundamental contained adequate information regarding requirements;
- The Privacy Fundamental displays the baseline requirements for stakeholders;
- The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
- The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
- The Privacy Fundamental should make available the text of GDPR requirements;
- The Privacy Fundamental should make available the text of NIST control requirements;
- The Privacy Fundamental could be merged with another Privacy Fundamental;
- The Privacy Fundamental would affect other controls should changes occur;
- Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
- The Privacy Fundamental is structed to act as independent control if necessary;

- On average those interviewed disagreed that:
  - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;

6.7 Data Subject Rights

The rights of the individuals follow directly or indirectly from the privacy principles and are requirements in the GDPR. An organisation must handle any requests of individuals with respect to their rights.

6.7.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.7.1*
Composability	The feedback for this interview category was: • There would be a perceived major benefit of directly linking to an existing framework by providing guidance on what is required for ensuring data subject rights are met; • The would be a benefit from an IT perspective to embed the data retention requirement into the design process
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding data subject rights; • The Business may require significant resources to create and implement a data subject rights; • It is critical that the business has clear and defined guidelines on how to meet these requirements
Maintainability	The feedback for this interview category was: • Currently the business provides two specific options for data subject;

	• A set of controls should be created and updated to ensure that data subject rights are always met

6.7.2 Proposed Business Requirement

- Risk #8.1: The project manager must ensure that subject rights are sufficiently covered by ensuring personal data can be retrieved / corrected / erased when needed.

6.7.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental contained adequate information regarding requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;
    - The Privacy Fundamental should make available the text of NIST control requirements;

  - The Privacy Fundamental could be merged with another Privacy Fundamental;
  - The Privacy Fundamental would affect other controls should changes occur;
  - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
  - Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
- On average those interviewed disagreed that:
  - The Privacy Fundamental is structed to act as independent control if necessary;

6.8 International Transfers

It is likely that an organisation will be required to process personal data outside the EU. It is often assumed that due to the GDPR, personal data cannot be processed outside the EU. This is not true. Personal data related to EU citizens can be processed outside the EU, either by the organisation itself or by a third party. The only condition is that the organisation takes certain defined measures to ensure that the personal data is treated with the same or similar protections as in the EU.

European organisations can transfer personal data to a third party in the following countries without any additional measures, as the GDPR is applies to these countries by way of a decision of the EEA Joint Committee: Iceland, Norway and Liechtenstein.

Additionally, transfers of personal data to a third party in the following countries without any additional measures, as the data protection laws in these countries are

deemed ‘’adequate’’ by the European Commission: Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

6.8.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.8.1*
Composability	The feedback for this interview category was: • There would be a benefit from an IT perspective to embed the international transfers requirements into the design process
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding international transfers;
Maintainability	The feedback for this interview category was: • Maintainability is fully focused on the legal aspects of GDPR, as decisions on accuracy and contractual requirements are provided at a legislative level;

6.8.2 Proposed Business Requirement

- Control #9.1: The responsible project manager must ensure Model Contract Clauses are executed between the third party and the organisation before personal data is transferred to the third party.
- Control #9.2: The responsible project manager must ensure a Data Protection Agreement is executed between the third party and the organisation before personal data is transferred to the third party.

6.8.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental contained adequate information regarding requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;
    - The Privacy Fundamental should make available the text of NIST control requirements;
    - The Privacy Fundamental would affect other controls should changes occur;
    - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
- On average those interviewed disagreed that:
    - The Privacy Fundamental is structed to act as independent control if necessary;

- Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
- The Privacy Fundamental could be merged with another Privacy Fundamental;

6.9 Third Party Processors

Organisations may engage a third party to process personal data on their behalf as part of a processing activity. This can include (but not limited to) the following: storage, transmission, access (including viewing personal data on a computer screen), access for maintenance purposes.

6.9.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.9.1*
Composability	The feedback for this interview category was: • There would be a benefit from a legal perspective to embed the third-party requirements into the contracting process • There would be a benefit from an IT perspective to embed the third-party requirements into the design process
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding international transfers;
Maintainability	• Requirements for third-party processors, whilst done at a request of a privacy practitioner, should be managed and maintained at a contracting level

6.9.2 Proposed Business Requirements

- Control #10.1: The responsible project manager must ensure Model Contract Clauses are executed between the third party and the organisation before personal data is transferred to the third party.
- Control #10.2: The responsible project manager must ensure a Data Protection Agreement is executed between the third party and the organisation before personal data is transferred to the third party.

6.9.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental contained adequate information regarding requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;
    - The Privacy Fundamental should make available the text of NIST control requirements;

- The Privacy Fundamental would affect other controls should changes occur;

- On average those interviewed disagreed that:
  - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
  - The Privacy Fundamental is structed to act as independent control if necessary;
  - Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
  - The Privacy Fundamental could be merged with another Privacy Fundamental;

6.10 Reporting

The privacy impact of reporting depends on the data that will be in the report and the subsequent use of that data.

6.10.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.10.1*
Composability	The feedback for this interview category was: • There would be a benefit from a legal perspective to embed the requirements to using personal data into the design process • There would be a benefit from an IT perspective to embed the reporting requirements into the design process
Reusability	The feedback for this interview category was:

	• The Business would benefit from having a set of pre-defined controls regarding reports and logs using personal data;
Maintainability	• Requirements will most likely remain flexible as reporting requirements and audiences are open to interpretation, and generally do not follow a set of standardly defined requirements

6.10.2 Proposed Business Requirement

- Control #11.1: reporting contains personal data require an established procedure to ensure reports are only used for a specific purpose.

6.10.3 Evaluation of Business Requirements

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental contained adequate information regarding requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;

- The Privacy Fundamental should make available the text of NIST control requirements;
- The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
- The Privacy Fundamental is structed to act as independent control if necessary;

- On average those interviewed disagreed that:
  - The Privacy Fundamental would affect other controls should changes occur;
  - Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
  - The Privacy Fundamental could be merged with another Privacy Fundamental;

6.11 Security Safeguard

Appropriate technical and organisational measures to ensure the security and integrity of personal data must be implemented.

6.11.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.11.1*
Composability	The feedback for this interview category was: • There would be a benefit from a legal perspective to embed the security requirements into the design process • There would be a benefit from an IT perspective to embed the security requirements into the design process

	• Ultimately whilst there is a requirement for security to be embedded into any system processing personal data, the assessment of security safeguard should be handled by security professional instead of privacy professionals
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding the requirement to have security assessed;
Maintainability	• Maintainability of these controls should be managed by those with knowledge of security controls with guidance from privacy professionals as to what would be adequate

6.11.2 Proposed Business Requirement

- Control #11.1: the responsible project manager must ensure that the organisations information security process is completed for all regions before any personal data can be processed (e.g. stored, transmitted or viewed) as part of this project.

6.11.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental contained adequate information regarding requirements;

- The Privacy Fundamental displays the baseline requirements for stakeholders;
- The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
- The Privacy Fundamental should make available the text of GDPR requirements;
- The Privacy Fundamental should make available the text of NIST control requirements;
- The Privacy Fundamental is structed to act as independent control if necessary;

- On average those interviewed disagreed that:
  - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
  - The Privacy Fundamental would affect other controls should changes occur;
  - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
  - Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
  - The Privacy Fundamental could be merged with another Privacy Fundamental;

6.12 Access

Access to personal data must be limited to those individuals that have a legitimate need to view the personal data. While proper access controls (a security measure) typically

require a clear access control framework, from a data protection perspective, it is important to review whether access to personal data is legitimate.

6.12.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.12.1*
Composability	The feedback for this interview category was: • There would be a benefit from a legal perspective to embed the access management requirements into the design process • There would be a benefit from an IT perspective to embed the access management requirements into the design process
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding access to personal data;
Maintainability	• Maintainability of these access security controls should be managed by those with knowledge of security controls with guidance from privacy professionals as to what would be adequate

6.12.2 Proposed Framework Control Description

- Control #12.1: the responsible project manager must ensure that access to personal data is limited to those that have a legitimate need to do so.

6.12.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:

- The format of the Privacy Fundaments effectively communicates the requirements;
- The Privacy Fundamental contained adequate information regarding requirements;
- The Privacy Fundamental displays the baseline requirements for stakeholders;
- The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
- The Privacy Fundamental should make available the text of GDPR requirements;
- The Privacy Fundamental should make available the text of NIST control requirements;
- The Privacy Fundamental is structed to act as independent control if necessary;
- The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;

- On average those interviewed disagreed that:
  - The Privacy Fundamental would affect other controls should changes occur;
  - The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
  - Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
  - The Privacy Fundamental could be merged with another Privacy Fundamental;

6.13 Works Councils

Whilst not a privacy fundamental it will be vital for organisations to take into account that labour laws in certain countries in Europe require either consultation with a local works council or approval of a local works council if personal data related to employees is processed.

6.13.1 Interview Feedback

Category	Question(s)
Compliance	• *Responses shown in Appendix 1.13.1*
Composability	The feedback for this interview category was: • There would be a benefit from a legal perspective to embed the works council requirements into the design process • There would be a benefit from an IT perspective to embed the works council requirements into the design process • There would be a benefit from a Labour Relations perspective to embed the works council requirements into the design process
Reusability	The feedback for this interview category was: • The Business would benefit from having a set of pre-defined controls regarding when labour relations are required to be involved prior to processing personal data;
Maintainability	• Maintainability of these labour relation controls should be managed by those within labour relations

6.13.2 Proposed Business Requirement

- Control #14.1: the responsible project manager must contact the Labour Relations team to consult with the central labour relations team in the EU regarding the processing of employee personal data

6.13.3 Evaluation of Proposed Privacy Fundamental

As shown in Appendix 2 the following observations have been made:

- On average those interviewed agreed that:
    - The format of the Privacy Fundaments effectively communicates the requirements;
    - The Privacy Fundamental contained adequate information regarding requirements;
    - The Privacy Fundamental displays the baseline requirements for stakeholders;
    - The format of the Privacy Fundamental could be reused for other Privacy Fundamentals;
    - The Privacy Fundamental should make available the text of GDPR requirements;
    - The Privacy Fundamental should make available the text of NIST control requirements;
    - The Privacy Fundamental is structed to act as independent control if necessary;
    - The Privacy Fundamental displays adequate information for stakeholders to implement the required controls;
- On average those interviewed disagreed that:

- The Privacy Fundamental would affect other controls should changes occur;
- The content of the Privacy Fundamental could be reused in additional Privacy Fundamentals;
- Additional Privacy Fundamentals could be drafted as a result or in support of this fundamental;
- The Privacy Fundamental could be merged with another Privacy Fundamental;

6.14 Other High Risks

Whilst the above list will cover the majority of processing activities within an average organisation, there are a number of activities which will require a further in-depth look as to how an individual's right to privacy may be affected:

- Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting.
- Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects\
- Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces.
- Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage
- Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

- Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified.
- Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage. Indeed, the personal and social consequences of the deployment of a new technology may be unknown.
- Preventing data subjects from exercising a right or using a service or a contract.

For these cases a more tailored and specific risk/control measure will have to be created, as these can be high risk situations which can also be open to interpretation

7. CONCLUSION

This thesis has provided an analytical overview of how both legal and information technology professionals can collaborate to create a privacy framework to aid with compliance and the implementation of systems which will process the personal data of individuals.

In the comparison of the leading privacy regulations implemented globally, we can see that the primary basis of these regulations is the European Union's General Data Protection Regulation. With any regulations building further upon this with appropriate amendments to allow for primarily public authorities to process personal data for purposes which may not have been covered by the legal bases within the General Data Protection Regulation. This regulation could, therefore, be seen as an appropriate

baseline to align any privacy compliance program to initially, then mature the program as required per additional regulation in scope.

As privacy regulations have become more prominent, the need for the professionals who understand the requirements of each regulation and how to translate them into understandable terms for use within an organisation has risen. In the information security field, the development of privacy risk frameworks has provided information technology professional with some high-level requirements for their systems and applications.

From further analysis of these requirements, we observe that while the controls provided themselves are relevant to the purposes required of them, without the context behind why these controls are necessary, the controls fail to provide more detail to those implementing systems regarding the risks associated with them, and the individual expectations from asserting their legal rights, a system developer may fail to understand the relevance importance of each control.

From the implementation chapter, the evaluation of each Privacy Fundamental shows that there, even after creating a framework to show what is required on a high, simple to understand, level there is still difference in opinion between legal, information technology, and privacy practitioners on what the adequate level of context that should be attached to a control.

7.1 Summary

By analysing the results of the feedback interviews conducted, we are able to draw a number of conclusions for the Privacy Fundamental artificats as a whole, and down to a level at which we can see which fundamentals received a higher average score than

others. Each question of the interviews resulted in five numberical scores within a range of one to five. From these results, the following observations have been made:

Highest level of agreement:

- Discoverability Q1 – "To what degree do you agree that related Privacy Fundamentals should be referenced in the content of this proposed Privacy Fundamental?" – This evaluation question resulted in the highest occurance of '5', with two of the Privacy Fundamentals scoring an average of 4.8 (PF7, PF8), and two scoring 4.6 (PF1, PF9);
- Standardisation Q2 – "To what degree does the content of the proposed Privacy Fundamental provide adequate information regarding requirements?"– This evaluation question resulted in the second highest occurances of '5', with two of the Privacy Fundamentals scoring an average of 4.8 (PF3, PF7), and one scoring 4.6 (PF13);

Lowest level of agreement:

- Composability Q2 - "To what degree to you agree this Privacy Fundamentals should be merged with another Privacy Fundamental?" This evaluation question resulted in the highest occurances of a score below 3, with three of the Privacy Fundamentals scoring an average of 2.2 (PF3, PF9, PF12), and two scoring 2.4 (PF10 and PF11);
- Autonomy Q1– "To what degree to you agree that significant change to the proposed Privacy Fundamental would affect other Privacy Fundamentals as a result?"– This evaluation question resulted in the second highest occurances of of a score below '3', with three of the Privacy Fundamentals scoring an average of 2 (PF2, PF3, PF11), and two scoring 2.4 (PF12 and PF13);

By analysing the results within these four evaluation questions, we see that there is agreement that the controls within the fundaments provide a baseline amount of information for stakeholders on how to implement their Privacy Fundamental requirements. The second most common observation is that the parties interviewed agree that the content of controls within a Fundamental should remain indepentant of eachother in order to prevent significant changes to additional controls in the event of any ammendments being required.

7.2 Future work

7.2.1 Suggested Future Topics

- The first suggestion would be to analyse further and compare on a larger scale of current and upcoming privacy regulations. As this thesis analysed only four privacy regulations worldwide, there is further potential to apply quantitative research methods to analyse trends in regulations to create a privacy framework for use before enforcement of future regulation.
- From observations within both the privacy regulations and the content of published privacy risk frameworks, there is little to no mention regarding an individual's expectation or analysis into what the actual risk to an individual's privacy is should a regulation or control mechanism not be implemented.
- Expansion of the created privacy framework to provide information about the criticality of each requirement. In general risk management terms, this could be regarding risk exposure, risk likelihood, and risk impact. With this information, an information technology professional can then prioritise during the development or implementation process.

- Expansion upon what is truly required for each control, by providing an example of implementations that may already exist within an organisation.

8. REFERENCES

Aldris, A., Nugroho, A., Lago, P., & Visser, J. (2013). Measuring the Degree of Service Orientation in Proprietary SOA Systems. *Proceedings - 2013 IEEE 7th International Symposium on Service-Oriented System Engineering.*

Cavoukain, A. (2011, January). *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices.* Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf

Cavoukain, A., & Jones Harbour, P. (2011, August). *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers.* Retrieved from https://collections.ola.org/mon/25008/312239.pdf

Denning, P. J. (1997). A New Social Contract for Research. *Communications of the ACM (40:2)*, 132-134.

European Parliament. (2016, 04 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council.* Retrieved from The European Parliament. (2016, April 27). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, a: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

Hevner, A. R., March, S. T., Park, J., & Sudha, R. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 76.

March, S. T., & Smith, G. (1995). Design and Natural Science Research on Information Technology. *Decision Support Systems (15:4)*, 251-266.

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A Design Theory for Systems that Support Emergent Knoweldge Processes. *MIS Quarterly (26:3)*, 179-212.

National Institute of Standards and Technology. (2020, 01 16). *NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management.* Retrieved from National Institute of Standards and Technology: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

Pereira Neto Macedo Advogados. (2018, 08 14). *Brazilian Data Protection Law (LGPD, English translation)*. Retrieved from IAPP: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

Philadelphia Convention. (1787, September 17). *The Constitution of the United States: A Transcription.* Retrieved from National Archives: https://www.archives.gov/founding-docs/constitution-transcript

Ryan Calo, M. (2010). The Boundaries of Privacy Harm. *Indiana Law Journal, vol. 86, no. 3*, 1131-1162.

Sabha, L., & Republic of India. (2019). *The Personal Data Protection Bill.* Retrieved from https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf

Silver, M. S., Markus, M. L., & Beath, C. M. (1995). The Information Technology Interaction Model: A Foundation for the MBA Core Course. *MIS Quarterly (19:3)*, 361-390.

Simon, H. A. (1996). The Sciences of the Artifical (3rd ed.). *MIT Press*.

State Constitution - Bill of Rights | NH.gov. (2018, December 5). Retrieved from https://www.nh.gov/glance/bill-of-rights.htm

State of Alaska. (1956, February 5). *Alaska's Constitution*. Retrieved from https://ltgov.alaska.gov/information/alaskas-constitution/

State of Arizona. (n.d). *Article 2 Section 8 - Right to privacy*. Retrieved from http://www.azleg.gov/const/2/8.htm

State of California. (1974, November 5). *Article I Declaration of Rights [Section 1 - Section 32]*. Retrieved from California Leglislative Information: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I

State of California. (2018). *1.81.5. California Consumer Privacy Act of 2018*. Retrieved from California Legislative Information: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

State of Hawaii. (1978, Novemeber 7). *State Constitution*. Retrieved from Legislative Reference Beurau: https://lrb.hawaii.gov/constitution#articlei

State of Illinois. (n.d). *Illinois Constitution - Article I*. Retrieved from http://www.ilga.gov/commission/lrb/con1.htm

State of Louisiana. (n.d). *Louisiana State Legislature Right to Privacy*. Retrieved from http://legis.la.gov/Legis/Law.aspx?d=206295

State of Montana. (1974, 11 05). *Montana Constitution, Article II, Section 10. Right of privacy*. Retrieved from https://web.archive.org/web/20131017202931/http://leg.mt.gov/bills/mca/Constition/II/10.htm

State of South Carolina. (n.d). *Constitution of the State of South Carolina*. Retrieved from http://www.scstatehouse.gov/scconstitution/a01.php

State of Washington. (n.d). *Code Reviser Washington State Constitution*. Retrieved from http://leg.wa.gov/CodeReviser/Pages/WAConstitution.aspx

The Florida Senate. (1980). *The Florida Constitution - The Florida Senate*. Retrieved from https://www.flsenate.gov/Laws/Constitution#A1S23

Tsichritzis, D. (1998). The Dynamics of Innovation. *Beyond Calculation: The Next Fifty Years of Computing*, 259-265.

U.S Department of Health, Education & Welfare. (1973, 06). *Report of Secretary's Advisory Comittee on Automated Personal Data Systems*. Retrieved from https://www.justice.gov/opcl/docs/rec-com-rights.pdf

Walls, J. G., Widmeyer, G. R., & El Sawry, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. *Information Systems Research (3:1)*, 36-59.

Westin, A. (1968). *Privacy And Freedom.* Retrieved from https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

What is the LGPD? Brazil's version of the GDPR - . . (2020). Retrieved from GDPR.eu: https://gdpr.eu/gdpr-vs-lgpd/

Zmud, R. (June 1997). Editors Comments. *MIS Quarterly (21:2)*, xxi-xxii.

9. Appendix 1 – CHAPTER 6 RESEARCH WORK

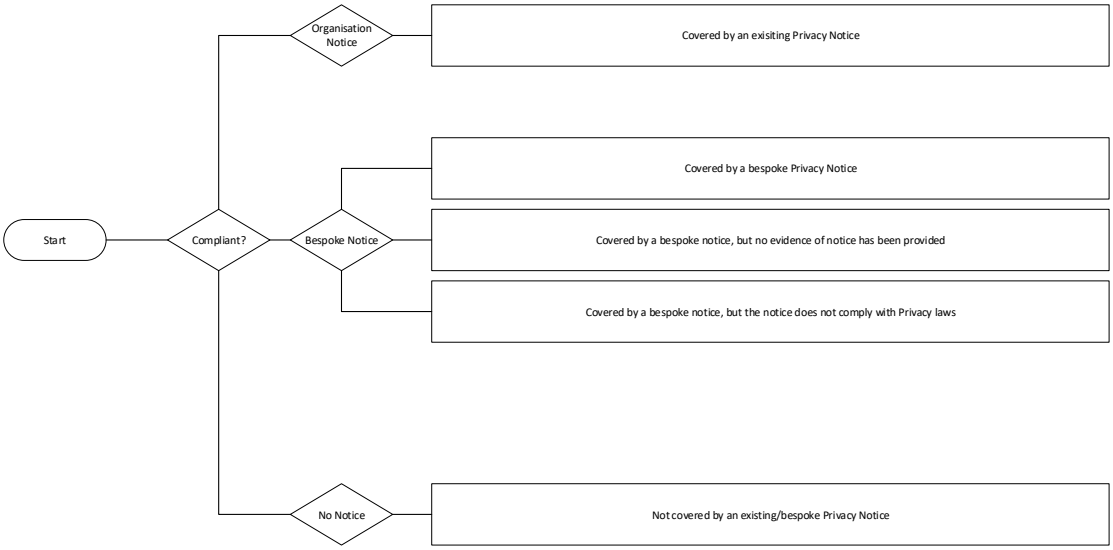
1.1 Transparency

This fundamental principle requires that an organisation is transparent with individuals as to the processing of their personal data. In order to comply with the transparency requirement of the GDPR, a privacy notice is typically provided to an individual. In practice, whether and how a privacy notice is provided will depend on the type of individuals and the personal data processed. In most cases, the processing activity will already be addressed in an existing data protection notice that has been provided to individuals. In limited situations a privacy notice specific to a processing activity will be necessary.

This description can then be further expanded on for specific target groups:

- Employees: employees are provided with a HR Privacy Notice. Most processing of personal data of employees will be covered under this notice This can be achieved in various ways, e.g. through emailing the impacted employees a bespoke notice or by posting a privacy notice on an interface for a new processing activity.
- Job applicants: job applicants are provided with a Privacy Notice. Most processing of personal data of job applicants will be covered under this notice. If the project's processing of personal data falls under this notice, there is no need for further action.
- Customers: have signed up to our terms and conditions, which includes reference to the Privacy Notice. Processing of personal data related to customers is generally covered in a privacy notice. In the event a project or processing activity is not covered by the organisational privacy notice, the privacy notice may need to be adapted.

1.1.1 Decision Tree



1.1.2 Proposed Framework Control Description

Fundamental	1: Transparency
Description	In order to comply with the transparency requirement of the GDPR, a privacy notice is typically provided to an individual.
GDPR Reference	Art. 5 GDPR Principles relating to processing of personal data Art. 12 GDP Transparent information, communication and modalities for the exercise of the rights of the data subject Art. 13 GDPR Information to be provided where personal data are collected from the data subject Art. 14 GDPR Information to be provided where personal data have not been obtained from the data subject
Business Requirement(s)	Control #1.1: the responsible 'project manager' must ensure that the project is in line with an existing privacy notice. Control #1.2: the responsible 'project manager' must ensure that a bespoke privacy notice is implemented. Control #1.3: the responsible 'project manager' must ensure the existing bespoke notice complies with applicable data protection laws. Control #1.4: the responsible 'project manager' must ensure that a copy of the existing bespoke privacy notice is provided to the privacy team.
NIST Reference	ID.BE-P1: The organization's role(s) in the data processing ecosystem is identified and communicated. ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated. GV.PO-P1: Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.

	CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event. CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.

1.2 Legal Ground

The processing of Personal Data is only lawful if and to the extent that at least one of the following legal grounds applies:

1. The individual has given consent to the processing of his or her Personal Data for one or more specific purposes.

2. The processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract.

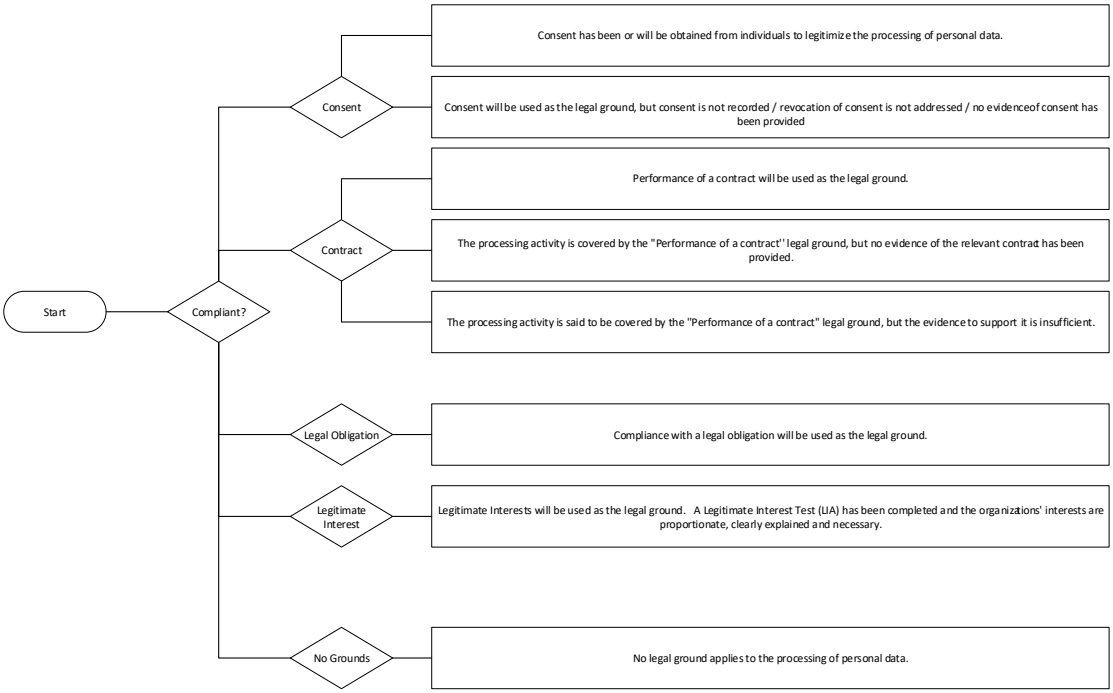
3. The processing is necessary for compliance with a legal obligation to which the organisation is subject.

4. The processing is necessary in order to protect the vital interests of the individual or another natural person.

5. The processing is necessary for the performance of a task carried out in the public interest or exercise of official authority vested.

6. The processing is necessary for the purposes of the legitimate interests pursued by an organisation or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.

1.2.1 Decision Tree



1.2.2 Proposed Framework Control Description

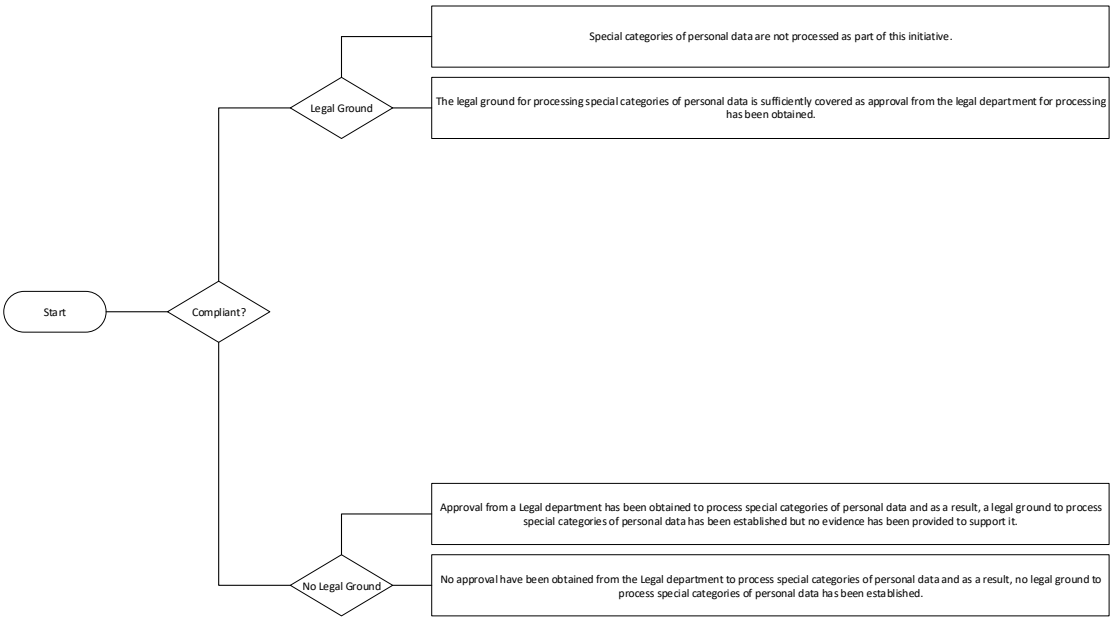
Fundamental	2: Legal Ground & Specific Purpose
Description	The processing of Personal Data is only lawful if at least one of the following legal grounds applies: • Consent of an Individual • Performance of a Contract • Legal Obligation(s) • Protection of the vital interest of an individual • Legitimate Interest of an Organisation
GDPR Reference	Art. 5 GDPR Principles relating to processing of personal data Art. 6 GDPR Lawfulness of processing Art. 7 GDPR Conditions for consent Art. 8 GDPR Conditions applicable to child's consent in relation to information society services Art. 35 GDPR Data protection impact assessment
Business Requirement(s)	Control #2.1: The processing activity is covered by compliance with a legal obligation. Control #2.2: The processing activity is covered by legitimate interests. A Legitimate Interest Test must be completed and the organisations interests must be proportionate, clearly explained and necessary. Control #2.3: The processing activity is covered by the 'performance of a contract'' legal ground, evidence of the relevant contract must be provided. Control #2.4: The processing activity is covered by the 'consent' legal ground, the project manager of the processing activity must

	ensure consent is recorded / ensure consent can be revoked by an individual / provide evidence of consent.
NIST Reference	CM.PO-P1: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place. CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established. CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences. ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).

1.3 Legal Ground for Processing Special Categories of Personal Data

Special categories of personal data are types of personal data that are deemed to be particularly sensitive, which warrants additional protections from a data protection perspective. Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. As a general rule, organisations should avoid processing special categories of personal data where possible.

1.3.1 Decision Tree



1.3.2 Proposed Framework Control Description

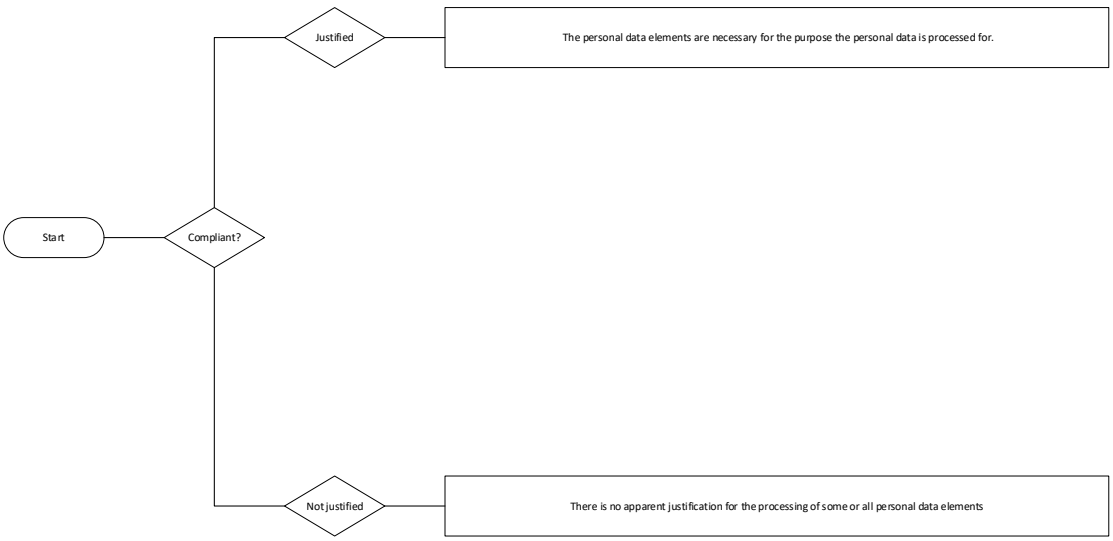
Fundamental	3: Legal Ground for Processing Special Categories of Personal Data
Description	Special categories of personal data are deemed to be particularly sensitive; this requires additional safeguards. Special categories of personal data are personal data revealing: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data, • biometric data; • health data; • sex life or sexual orientation.
GDPR Reference	Art. 5 GDPR Principles relating to processing of personal data Art. 9 GDPR Processing of special categories of personal data Art. 10 GDPR Processing of personal data relating to criminal convictions and offences Art. 35 GDPR Data protection impact assessment
Business Requirement(s)	Control #3.1: The IT / Business Owner must obtain approval from the legal department prior to processing special categories of personal.
NIST Reference	ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).

1.4 Data Minimization & Purpose Limitation

Organisations are only allowed to process Personal Data that are adequate, relevant and strictly necessary for the purposes the organisation is processing the Personal Data for. This is a basic principle that is often difficult to comply with since Data Protection Law is not specific on what categories of Personal Data (or the documents containing Personal Data) companies are allowed to use. The organisation is responsible to make this assessment on a case by case basis. If there is a less privacy invasive way to process Personal Data, e.g. by using pseudonymized Personal Data or anonymous data, that should be the preferred approach and greatly adds to privacy by design and default principles. However, using such techniques is not always possible due to technical or cost restraints.

Practically speaking, the assessment of this requirement is best done by challenging the organisation on data elements that seem out of place or unnecessary for the purposes is processing the Personal Data for.

1.4.1 Decision Tree



1.4.2 Proposed Framework Control Description

Fundamental	4: Data Minimization & Purpose Limitation

Description	Personal Data that is to be processed must be adequate, relevant and strictly necessary for the purposes the organisation is processing the Personal Data for.
GDPR Reference	Art. 5 GDPR Principles relating to processing of personal data Art. 35 GDPR Data protection impact assessment
Business Requirement(s)	Control #4.1 The project manager must justify the processing of such personal data elements by specifying why these data elements are strictly necessary for execution of the processing activity. If no justification is provided, the project cannot process such personal data elements
NIST Reference	ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried. ID.IM-P5: The purposes for the data actions are inventoried. ID.IM-P6: Data elements within the data actions are inventoried. ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services. ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties). ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk. ID.RA-P3: Potential problematic data actions and associated problems are identified.

1.5 Data Accuracy

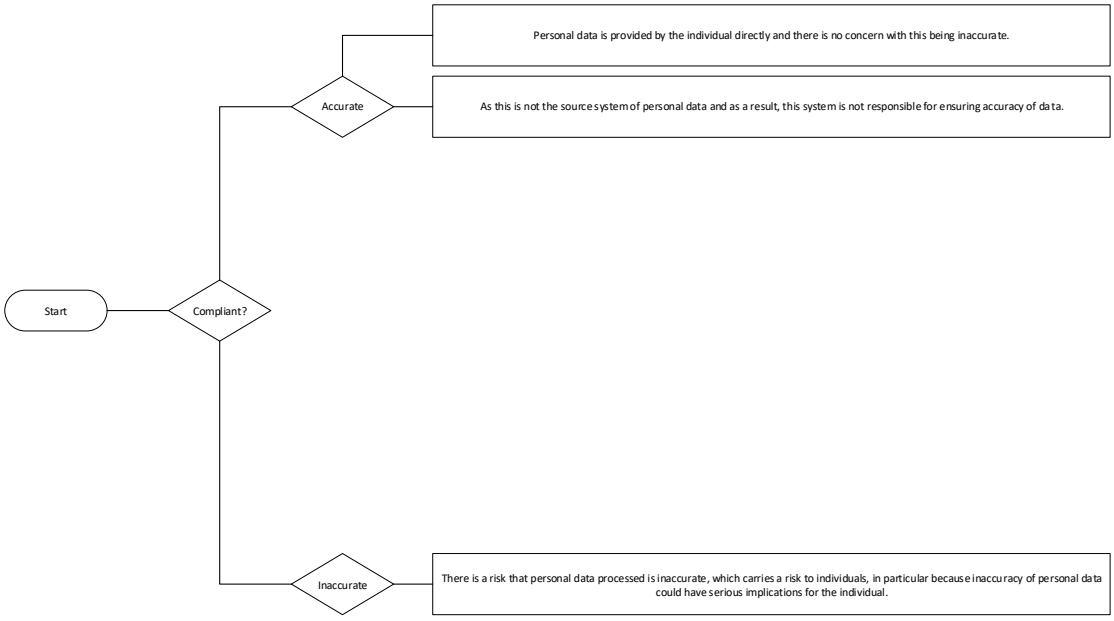
Personal data need to be accurate and kept up to date. Organisations must take reasonable steps to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. The GDPR does not define the word ‘accurate’.

What an organisation uses Personal Data for may affect whether it is accurate or not. For example, just because personal data has changed doesn’t mean that a historical record is inaccurate. For example, the fact that a customer changes their address does not mean that a record of deliveries to the old address of a customer must be erased or updated.

It may be impractical to check the accuracy of personal data someone else provides. In order to ensure that records are not inaccurate or misleading in this case, organisations must:

- accurately record the information provided;
- accurately record the source of the information;
- take reasonable steps in the circumstances to ensure the accuracy of the information; and
- carefully consider any challenges to the accuracy of the information.

1.5.1 Decision Tree



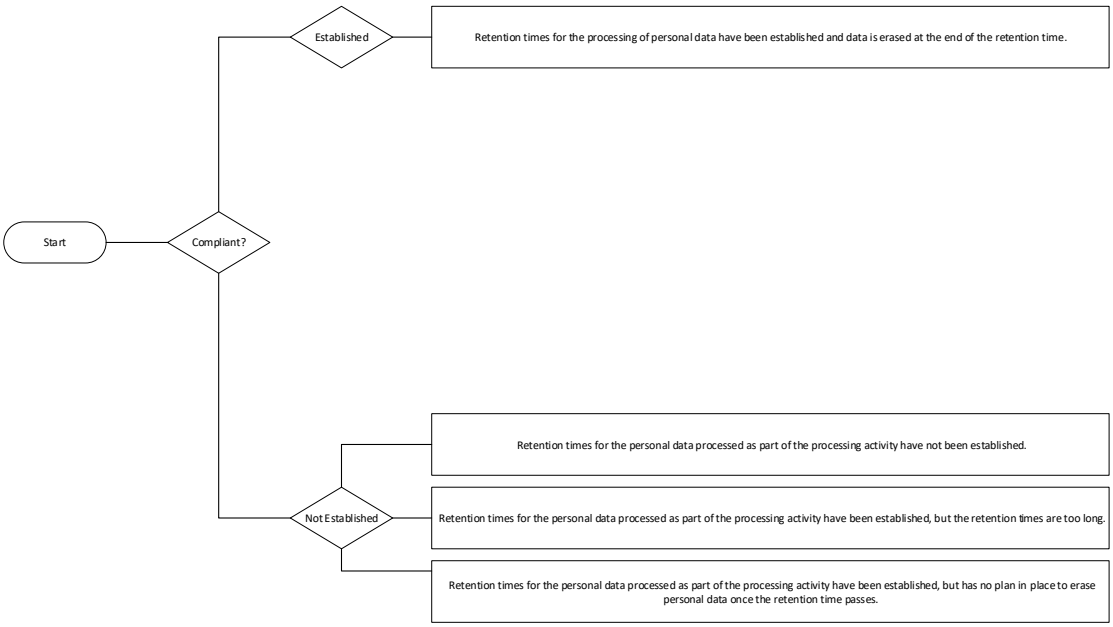
1.5.2 Proposed Framework Control Description

Fundamental	5: Data Accuracy
Description	Personal data need to be accurate and kept up to date.
GDPR Reference	Art. 5 GDPR Principles relating to processing of personal data Art. 35 GDPR Data protection impact assessment
Business Requirement(s)	Control #5.1 The project manager must ensure capabilities to ensure the accuracy of personal data are implemented. Control #5.2 The project manager must ensure capabilities to remove personal data are implemented.
NIST Reference	CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place. CT.DM-P1: Data elements can be accessed for review. CT.DM-P2: Data elements can be accessed for transmission or disclosure. CT.DM-P3: Data elements can be accessed for alteration. CT.DM-P4: Data elements can be accessed for deletion.

1.6 Retention

Organisations are only allowed to process Personal Data as long as necessary to serve the purpose of processing those Personal Data. This is a broad requirement, whereby the law does not specify the exact required retention time for personal data. While there is guidance from regulators on retention times for certain types of personal data (e.g. CCTV footage, personal data related to job applicants), most retention times for personal data will depend on the circumstances of the specific processing activity and applicable laws that specify minimum retention times.

1.6.1 Decision Tree



1.6.2 Proposed Framework Control Description

Fundamental	6: Retention
Description	Personal Data is only allowed to processed as long as necessary to serve the specific purpose of processing.
GDPR Reference	Art. 11 GDPR Processing which does not require identification
Business Requirement(s)	Risk #6.1: project manager must establish retention times for the personal data processed as part of the processing activity.

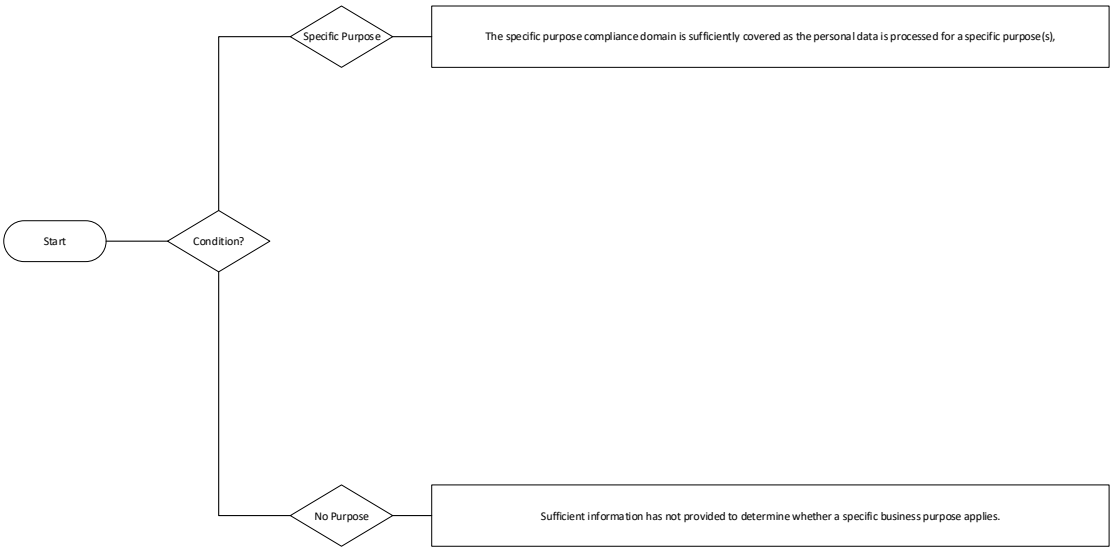
NIST Reference	GV.PO-P1: Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.

1.7 Data Subject Rights

The rights of the individuals follow directly or indirectly from the privacy principles and are requirements in the GDPR. An organisation must handle any requests of individuals, e.g. our customers and employees with respect to their rights. In short, the rights of individuals are the right to information, access, rectification, erasure, restriction, data portability and objection. The right to objection may imply that organisations must stop Personal Data processing to the extent we need to reply to the request. Organisations need to take into account or implement the individuals' rights in our processes or systems.

From a practical perspective, it can be challenging to implement technical measures to ensure a processing activity can action certain requests from individuals. For example, the erasure of data can be challenging to implement. At the same time, often data subject rights do not play a big role in a processing activity.

1.7.1 Decision Tree



1.7.2 Proposed Framework Control Description

Fundamental	7: Data Subject Rights
Description	An organisation must handle any requests of individuals with respect to their rights. The rights of individuals are: • the right to information; • the right to access; • the right to rectification; • the right to erasure; • the right to restriction; • the right to data portability; • the right to objection;
GDPR Reference	Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject Art. 15 GDPR Right of access by the data subject Art. 16 GDPR Right to rectification Art. 17 GDPR Right to erasure ('right to be forgotten') Art. 18 GDPR Right to restriction of processing Art. 19 GDPR Notification obligation regarding rectification or erasure of personal data or restriction of processing Art. 20 GDPR Right to data portability Art. 21 GDPR Right to object Art. 22 GDPR Automated individual decision-making, including profiling Art. 23 GDPR Restrictions Art. 34 GDPR Communication of a personal data breach to the data subject Art. 35 GDPR Data protection impact assessment
Business Requirement(s)	Risk #8.1: The project manager must ensure that subject rights are sufficiently covered by ensuring personal data can be retrieved / corrected / erased when needed.

NIST Reference	GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place. CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention). CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place. CT.DM-P1: Data elements can be accessed for review. CT.DM-P2: Data elements can be accessed for transmission or disclosure. CT.DM-P3: Data elements can be accessed for alteration. CT.DM-P4: Data elements can be accessed for deletion. CT.DM-P5: Data are destroyed according to policy. CT.DM-P6: Data are transmitted using standardized formats. CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.

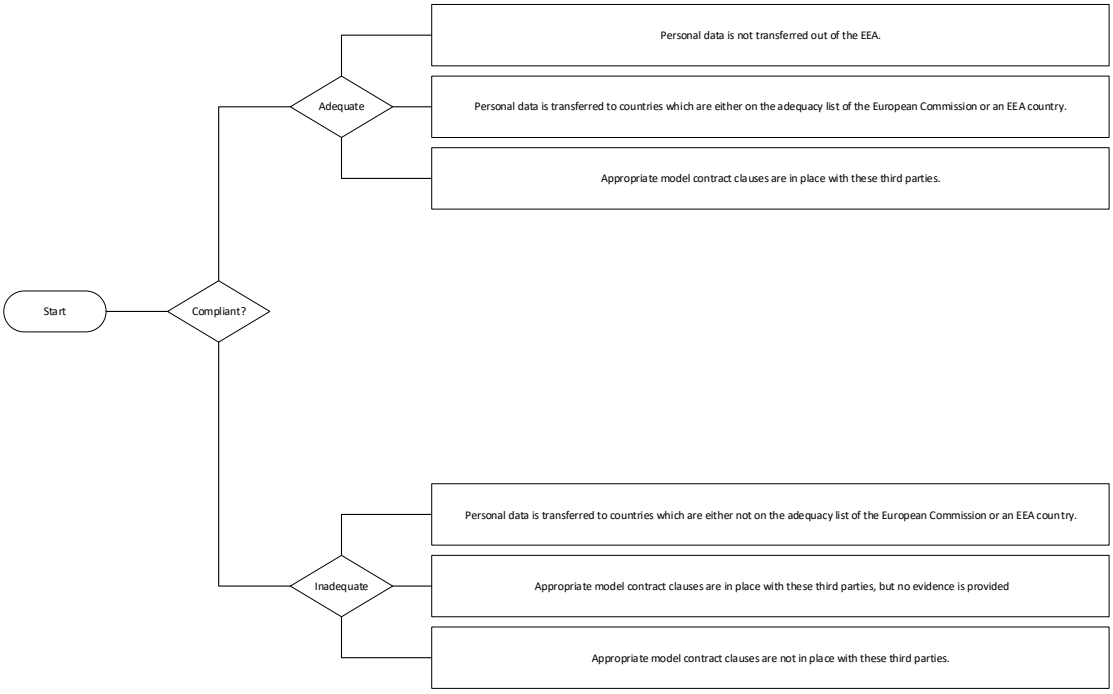
1.8 International Transfers

It is likely that an organisation will be required to process personal data outside the EU. It is often assumed that due to the GDPR, personal data cannot be processed outside the EU. This is not true. Personal data related to EU citizens can be processed outside the EU, either by the organisation itself or by a third party. The only condition is that the organisation takes certain defined measures to ensure that the personal data is treated with the same or similar protections as in the EU.

European organisations can transfer personal data to a third party in the following countries without any additional measures, as the GDPR is applies to these countries by way of a decision of the EEA Joint Committee: Iceland, Norway and Liechtenstein.

Additionally, transfers of personal data to a third party in the following countries without any additional measures, as the data protection laws in these countries are deemed ‘’adequate’’ by the European Commission: Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

1.8.1 Decision Tree



1.8.2 Proposed Framework Control Description

Fundamental	8: International Transfers
Description	An organisation must legitimise any transfer of personal data if processing takes processing takes place outside of the EEA or in a country without an Adequacy Decision.
GDPR Reference	Art. 27 GDPR Representatives of controllers or processors not established in the Union Art. 44 GDPR General principle for transfers Art. 45 GDPR Transfers on the basis of an adequacy decision Art. 46 GDPR Transfers subject to appropriate safeguards Art. 47 GDPR Binding corporate rules Art. 48 GDPR Transfers or disclosures not authorised by Union law Art. 49 GDPR Derogations for specific situations Art. 50 GDPR International cooperation for the protection of personal data
Business Requirement(s)	Control #9.1: The responsible project manager must ensure Model Contract Clauses are executed between the third party and the organisation before personal data is transferred to the third party. Control #9.2: The responsible project manager must ensure a Data Protection Agreement is executed between the third party and the organisation before personal data is transferred to the third party.
NIST Reference	ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).

1.9 Third Party Processors

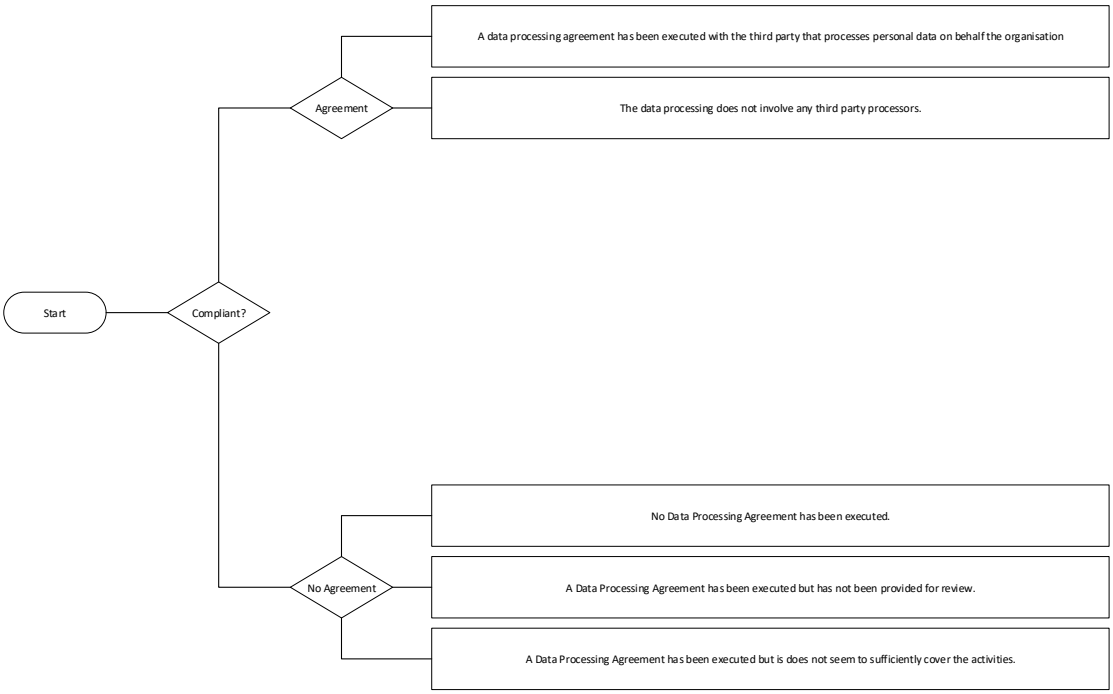
Organisations may engage a third party to process personal data on their behalf as part of a processing activity. This can include (but not limited to) the following: storage, transmission, access (including viewing personal data on a computer screen), access for maintenance purposes. In the cases case where a third-party processes personal data on behalf of an organisation, the agreement with the third party must contain, as a minimum, the required contractual obligations stipulated in the GDPR.

This can be addressed through one of the following means, depending on the risk associated with the processing of personal data by a third party:

Data processing agreement (DPA). The DPA is an extensive data protection related agreement and suitable for all processing activities, in particular for global projects and projects that involve either special categories of personal data or large volumes of personal data.

Standard Contractual Clauses is the most basic form of compliance with the requirements of the GDPR and suitable for the most basic processing of personal data, such as name and email address.

1.9.1 Decision Tree



1.9.2 Proposed Framework Control Description

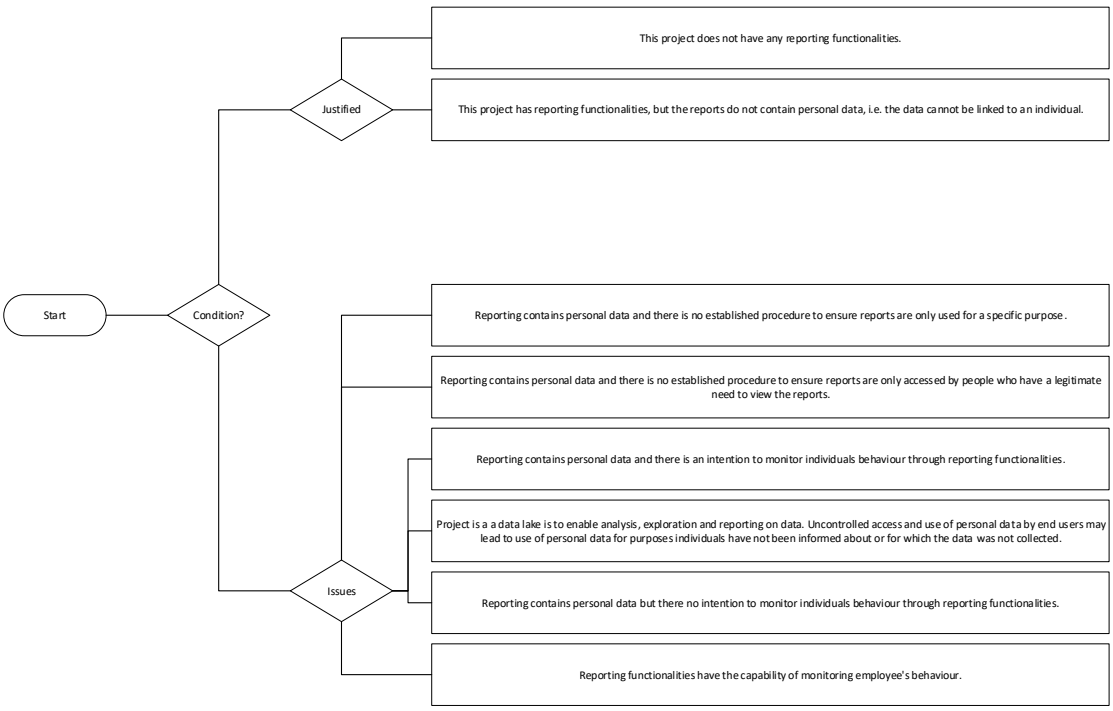
Fundamental	9: Third Party Processors
Description	All third-party processing activities involving personal data, including, but not limited to: • Storage; • Transmission; • Access; • Deletion; Must be subject to an agreement between the both parties, this can be achieved by: • A Data Processing Agreement • Standard Contractual Clauses

GDPR Reference	Art. 24 GDPR Responsibility of the controller Art. 26 GDPR Joint controllers Art. 27 GDPR Representatives of controllers or processors not established in the Union Art. 28 GDPR Processor rt. 29 GDPR Processing under the authority of the controller or processor
Business Requirement(s)	Control #10.1: The responsible project manager must ensure Model Contract Clauses are executed between the third party and the organisation before personal data is transferred to the third party. Control #10.2: The responsible project manager must ensure a Data Protection Agreement is executed between the third party and the organisation before personal data is transferred to the third party.
NIST Reference	ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties). ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services. ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process. ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program. ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations. GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.

6.10 Reporting

Reporting functionalities of a tool or project are often overlooked. However, reporting can lead to privacy risks that impact Individuals. For example: a facility has access gates where employees obtain access by means of a personal access badge. These gates are driven by a computer program that can run reports on the exact time and date an employee has entered the building. The reporting in itself is not privacy invasive – rather, what is subsequently done with the report is relevant. If the report in this example is used to monitor employees to see whether they arrive on time at work, there is a privacy impact. If the reports are used to determine how many people are in the building in case of a fire, the privacy impact is negligible. So, the privacy impact depends on the data that will be in the report and the subsequent use of that data.

1.10.1 Decision Tree



1.10.2 Proposed Framework Control Description

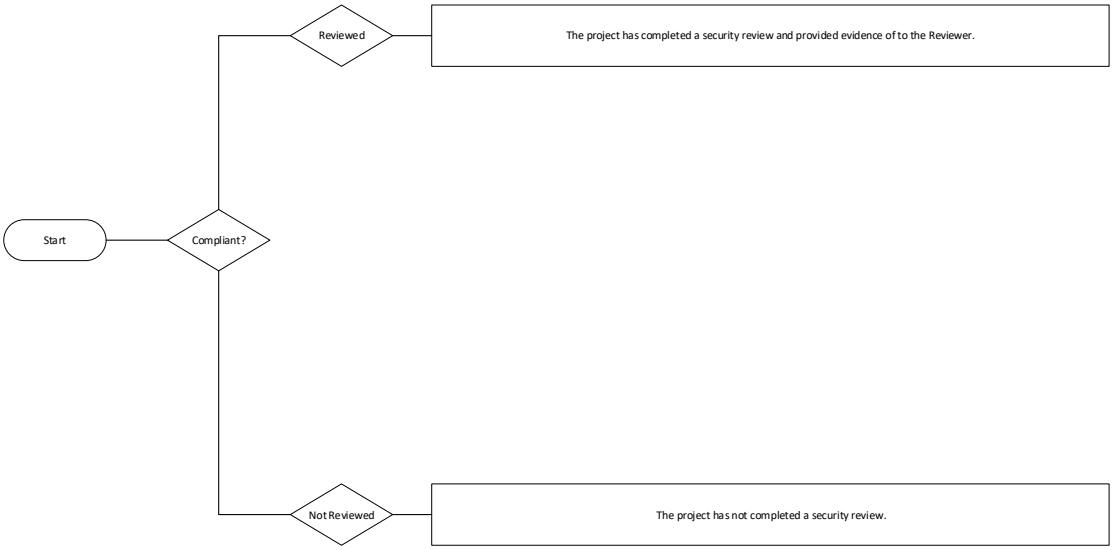
Fundamental	10: Reporting

Description	Reports containing personal data must be used for a specific purpose and accessed by those with a legitimate purpose for viewing.
GDPR Reference	Art. 5 GDPR Principles relating to processing of personal data Art. 35 GDPR Data protection impact assessment
Business Requirement(s)	Risk #11.1: reporting contains personal data require an established procedure to ensure reports are only used for a specific purpose.
NIST Reference	ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias. CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization). CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behaviour or activities (e.g., data processing is decentralized, distributed architectures).

1.11 Security Safeguard

One of the key aspects of data protection compliance is to implement appropriate technical and organisational measures to ensure the security and integrity of personal data. Organisations should implement a process to review the security controls of new and existing processing activities. This process should consist of a systematic review of the security controls associated with a data processing.

1.11.1 Decision Tree



1.11.2 Proposed Framework Control Description

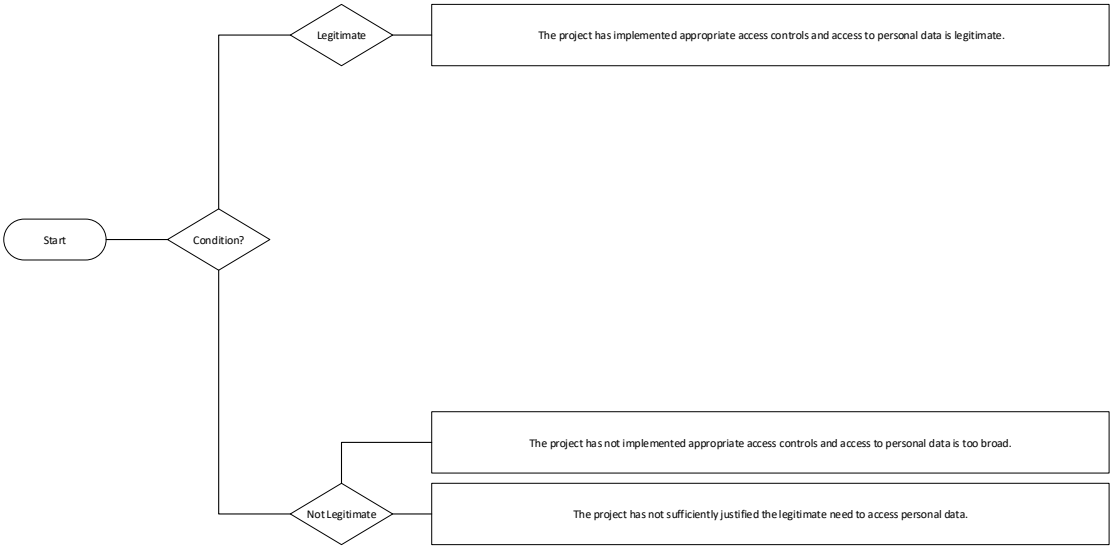
Fundamental	11: Security Safeguard
Description	Appropriate technical and organisational measures to ensure the security and integrity of personal data must be implemented before processing
GDPR Reference	Art. 5 GDPR Principles relating to processing of personal data Art. 32 GDPR Security of processing Art. 33 GDPR Notification of a personal data breach to the supervisory authority
Business Requirement(s)	Control #11.1: the responsible project manager must ensure that the organisations information security process is completed for all regions before any personal data can be processed (e.g. stored, transmitted or viewed) as part of this project.
NIST Reference	CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed. CT.DP-P1: Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).

	CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements. PR.PO-P1: A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality). PR.PO-P2: Configuration change control processes are established and in place. PR.PO-P3: Backups of information are conducted, maintained, and tested. PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met. PR.PO-P5: Protection processes are improved. PR.PO-P6: Effectiveness of protection technologies is shared. PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. PR.PO-P8: Response and recovery plans are tested. PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening). PR.PO-P10: A vulnerability management plan is developed and implemented. PR.DS-P1: Data-at-rest are protected. PR.DS-P2: Data-in-transit are protected PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition. PR.DS-P4: Adequate capacity to ensure availability is maintained. PR.DS-P5: Protections against data leaks are implemented. PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity. PR.DS-P7: The development and testing environment(s) are separate from the production environment. PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity. PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. PR.PT-P1: Removable media is protected and its use restricted according to policy. PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. PR.PT-P3: Communications and control networks are protected. PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

1.12 Access

Access to personal data must be limited to those individuals that have a legitimate need to view the personal data. While proper access controls (a security measure) typically require a clear access control framework, from a data protection perspective, it is important to review whether access to personal data is legitimate.

1.12.1 Decision Tree



1.12.2 Proposed Framework Control Description

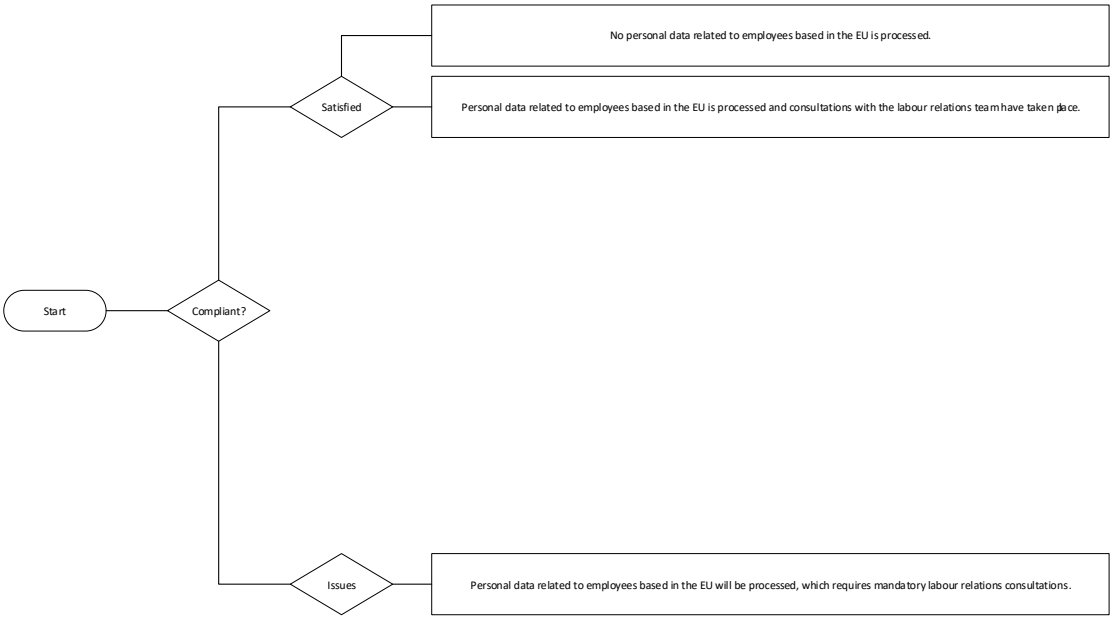
Fundamental	12: Access
Description	Access to personal data must be limited to those individuals that have a legitimate need to view the personal data.
GDPR Reference	Art. 5 GDPR Principles relating to processing of personal data
Business Requirement(s)	Control #12.1: the responsible project manager must ensure that access to personal data is limited to those that have a legitimate need to do so.
NIST Reference	GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy. GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners). GV.AT-P1: The workforce is informed and trained on its roles and responsibilities PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

	PR.AC-P2: Physical access to data and devices is managed. PR.AC-P3: Remote access is managed. PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation). PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks). PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

1.13 Works Councils

Whilst not a privacy fundamental it will be vital for organisations to take into account that labour laws in certain countries in Europe require either consultation with a local works council or approval of a local works council if personal data related to employees is processed.

1.13.1 Decision Tree



1.13.2 Proposed Framework Control Description

Fundamental	13: Works Councils

Description	Works Councils consultation is required if personal data related to employees is processed.
GDPR Reference	N/A
Business Requirement(s)	Control #14.1: the responsible project manager must contact the Labour Relations team to consult with the central labour relations team in the EU regarding the processing of employee personal data
NIST Reference	N/A

10. Appendix 2 – Table of Evaluation Interview Results

Question Number	Question	Privacy Fundamental Number												
		PF1	PF2	PF3	PF4	PF5	PF6	PF7	PF8	PF9	PF10	PF11	PF12	PF13
Standardisation Q1	To what degree does the format of the proposed Privacy Fundamental effectively communicate the requirements?	5	5	5	5	5	5	5	5	5	5	5	5	5
		4	4	4	4	4	4	4	4	4	4	4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4
		3	3	3	3	3	3	3	3	3	3	3	3	3
		3	3	3	3	3	3	3	3	3	3	3	3	3
	Average Score:	3.8	3.8	3.8	3.8	3.8	3.8	3.8	3.8	3.8	3.8	3.8	3.8	3.8
Standardisation Q2	To what degree does the content of the proposed Privacy Fundamental provide adequate information regarding requirements?	4	4	5	3	4	5	5	5	4	4	4	4	5
		4	4	5	4	4	5	5	5	4	4	4	4	5
		4	4	4	3	4	4	5	4	4	4	4	4	5
		2	3	5	2	2	3	4	4	2	4	2	4	4
		3	3	5	2	1	3	5	3	3	4	2	4	4
	Average Score:	3.4	3.6	4.8	2.8	3	4	4.8	4.2	3.4	4	3.2	4	4.6

Abstraction Q1	To what degree can the proposed Privacy Fundamental be published to provide only the base line requirements expected from the stakeholders?	4	4	5	4	4	4	4	5	4	4	4	5	5
		3	4	5	4	3	4	5	4	4	4	4	4	5
		4	3	5	3	3	4	4	5	4	4	4	4	4
		3	3	4	2	2	2	3	4	3	3	2	4	4
		4	3	4	2	2	2	2	4	3	3	3	3	4
	Average Score:	3.6	3.4	4.6	3	2.8	3.2	3.6	4.4	3.6	3.6	3.4	4	4.4
Abstraction Q2	To what degree do you agree that the proposed Privacy Fundamental provides enough information for stakeholders to implement requirements?	4	3	5	3	4	3	4	4	4	3	4	4	5
		4	4	4	3	4	3	5	4	3	3	3	5	5
		3	4	4	3	3	2	5	4	3	4	3	4	5
		2	2	4	2	2	2	3	4	2	4	2	2	5
		3	2	4	2	1	2	1	4	2	3	1	4	4
	Average Score:	3.2	3	4.2	2.6	2.8	2.4	3.6	4	2.8	3.4	2.6	3.8	4.8
Loose Coupling Q1	To what degree is the proposed Privacy Fundamental structured to act independently from other Privacy Fundamentals or requirements?	5	3	4	3	4	4	3	3	2	4	4	4	5
		5	3	5	3	4	4	3	3	2	4	5	4	5
		4	3	4	4	4	4	2	2	3	4	4	4	5
		3	3	4	2	3	3	3	3	3	2	3	4	4
		4	3	4	2	3	3	3	3	3	3	3	4	4
	Average Score:	4.2	3	4.2	2.8	3.6	3.6	2.8	2.8	2.6	3.4	3.8	4	4.6

Autonomy Q1	To what degree to you agree that significant change to the proposed Privacy Fundamental would affect other Privacy Fundamentals as a result?	5	2	1	2	3	4	4	4	4	2	1	2	4
		4	1	2	2	3	4	5	4	4	3	1	2	2
		5	2	1	3	3	3	5	5	3	3	2	2	2
		4	3	3	3	3	3	3	3	3	3	3	3	2
		3	2	3	3	3	3	4	3	3	3	3	3	2
	Average Score:	4.2	2	2	2.6	3	3.4	4.2	3.8	3.4	2.8	2	2.4	2.4
Genericity Q1	To what degree do you agree that the format of the proposed Privacy Fundamental can be reused?	4	4	4	4	4	4	4	4	4	4	4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4
		5	5	5	5	5	5	5	5	5	5	5	5	5
		4	4	4	4	4	4	4	4	4	4	4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4
	Average Score:	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
Genericity Q2	To what degree do you agree that the requirements of the proposed Privacy Fundamental can be reused in additional Fundamentals?	4	4	4	4	4	4	4	5	4	5	1	2	4
		4	4	4	4	4	5	5	4	4	5	1	1	4
		5	4	5	4	3	4	4	4	5	4	2	2	2
		2	3	3	3	3	4	4	3	3	4	2	3	2
		4	4	3	3	3	3	3	4	4	4	2	3	2
	Average Score:	3.8	3.8	3.8	3.6	3.4	4	4	4	4	4.4	1.6	2.2	2.8

Discoverability Q1	To what degree do you agree that related Privacy Fundamentals should be referenced in the content of this proposed Privacy Fundamental?	4	4	4	3	5	4	5	5	5	5	4	4	3
		5	5	4	4	4	4	5	5	5	5	4	4	3
		4	5	4	3	5	3	5	5	4	4	4	4	3
		5	4	4	4	4	5	5	5	4	4	5	5	3
		5	4	4	4	4	4	4	4	5	4	5	5	3
	Average Score:	4.6	4.4	4	3.6	4.4	4	4.8	4.8	4.6	4.4	4.4	4.4	3
Discoverability Q2	To what degree that the referenced GDPR Requirements should be made available as part of the proposed Privacy Fundamental?	4	4	4	4	4	4	4	4	4	4	4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4
		5	5	5	5	5	5	5	5	5	5	5	5	5
		4	4	4	4	4	4	4	4	4	4	4	4	4
	Average Score:	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
Discoverability Q3	To what degree that the referenced NIST Controls should be made available as part of the proposed Privacy Fundamental?	3	3	3	3	3	3	3	3	3	3	3	3	3
		4	4	4	4	4	4	4	4	4	4	4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4
		5	5	5	5	5	5	5	5	5	5	5	5	5
		5	5	5	5	5	5	5	5	5	5	5	5	5
	Average Score:	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2

Composability Q1	To what degree to you agree that new Privacy Fundamentals could be drafted as a result of this proposed Privacy Fundamental?	4	5	2	2	3	4	4	2	2	2	2	2	1
		4	5	2	2	3	4	4	2	2	2	2	2	1
		3	4	1	3	3	3	4	3	1	2	2	2	2
		3	3	3	3	3	3	3	3	3	3	3	2	2
		3	3	3	3	3	3	3	3	3	3	3	3	2
	Average Score:	3.4	4	2.2	2.6	3	3.4	3.6	2.6	2.2	2.4	2.4	2.2	1.6
Composability Q2	To what degree to you agree this Privacy Fundamentals should be merged with another Privacy Fundamental?	4	4	4	1	4	4	4	2	2	3	2	1	4
		3	4	4	1	4	4	3	1	4	2	2	1	2
		4	5	3	2	3	3	5	2	2	2	2	2	2
		3	3	3	3	3	4	4	3	3	3	3	3	3
		3	4	3	3	3	3	4	3	3	3	3	3	3
	Average Score:	3.4	4	3.4	2	3.4	3.6	4	2.2	2.8	2.6	2.4	2	2.8