Global Information Assurance Certification Paper

Next Generation of Privacy in Europe and the Impact on Information Security: Complying with the GDPR

GIAC (GLEG) Gold Certification

Author: Ed Yuwono, Ed.Yuwono.MSISM@gmail.com
Advisor: Manuel Humberto Santander Pelaez
Accepted: December 2nd, 2016
Template Version September 2014

Abstract

Human rights have a strong place within Europe, part of this includes the fundamental right to privacy. Over the years, individual privacy has strengthened through various European directives. With the evolution of privacy continuing in Europe through the release of the General Data Protection Regulation (GDPR), how will the latest iteration of European Union (EU) regulation affect organisations and what will information security leaders need to do to meet this change? This paper will explore the evolution of privacy in Europe, the objectives and changes this iteration of EU privacy regulation will provide, what challenges organisations will experience, and how information security could be leveraged to satisfy the regulation.

*Note this is not a substitute for legal advice, always seek advice from legal counsel prior to commencing with this project.

1. Introduction

The right for privacy across Europe originated in response to human rights abuses during World War 2. Privacy International defines the human right of privacy as, "*a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.* " (Privacy International, n.d.). In 1950, European nations adopted the European Convention of Human Rights (ECHR) to provide unity among European nations through the respect of human rights and freedoms (ECHR, 2010). Article 8 of the ECHR provides the right to respect for one's "*private and family life, his home and his correspondence*" (ECHR, 2010).

Following the introduction of the ECHR, nations adopted various privacy laws to protect their citizens. In 1970, the German state of Hesse introduced the first-ever data protection law (Burkert, 2000). In 1978, France became an early adopter of a national privacy law after the public reaction to a government plan to link administrative data to identify citizens (Deutsche Welle, 2011).

As more nations adopted privacy laws, this introduced a legal imbalance between European nations (Burkert, 2000). Legal imbalances meant that entities such as organisations or government departments based in nations with strong privacy legislation would refuse to transfer data to entities based in nations with inadequate protection. The imbalance resulted in entities initiating legal challenges against organisations opposing the transfer of their citizen's data. These legal imbalances became evident after Sweden stopped the transfer of personal data of Swedes to the UK in the absence of adequate data protection laws (Burkert, 2000).France also blocked data transfers of French citizens to Italy (Newman, 2008). Privacy imbalances affected everything from border security to medical research, which resulted in the European Commission realising that the need for uniform data privacy was important for organisations to operate across borders (Newman, 2008).

To resolve the imbalance, the European Commission standardised legislation on data protection in 1995 through the Data Protection Directive 95/46/EC (European Parliament, 1995). Soon after, Member States transposed this directive into their respective legislation only to re-introduce legislation fragmentation between European

Union members (European Parliament, 2016). The results from fragmentation meant that organisations in one Member State might not be able to transfer data due to different privacy laws of other Member States.

Superseding the Data Protection Directive, the General Data Protection Regulation (GDPR) aims to re-standardise data protection rights of EU citizens, strengthen data protection laws across Europe, and simplify the regulatory environment for businesses (European Parliament, 2016; European Commission, 2016). The significance of GDPR should not be underestimated as it impacts any organisation located anywhere in the world that processes data on European citizens. Non-compliance with the GDPR could see entities incur enormous fines forcing organisations to reconsider how they handle citizen data on Europeans.

1.1. Document Tenets

A working group led by the Centre for Information Policy Leadership highlighted several challenges with implementing the GDPR (Centre for Information Policy Leadership, 2016). These challenges include: re-introducing fragmentation in privacy legislation as the Member States implement their derogations, the absence of guidance for GDPR implementation, and the requirement for further collaboration between policy makers (Centre for Information Policy Leadership, 2016).

While the GDPR is a 2nd generation regulation, there are new sections in this regulation that are subject to further interpretation. The open-ended nature of the GDPR is intended to allow evolutionary processes to mould the regulation, such examples include member state interpretation, new developments in technology and future case law. Hence, the GDPR must be part of an organisation's strategic plan set at a governance level. A recent survey on the state of European Data Privacy uncovered major cultural deficiencies within organisations that serve against the GDPR (SC Magazine UK, 2016; Symantec, 2016). Some organisations surveyed were out of touch with consumers, didn't consider compliance a priority and underestimated the effort required to comply (Symantec, 2016). The GDPR requires a cultural shift demanding accountability from staff from all levels throughout the entire organisation to achieve compliance.

The emphasis of this document is to operate within legal boundaries of the regulation by demonstrating that an organisation is taking verifiable steps to protect the privacy of European Citizens. This document will provide opportunities for organisations to align with the spirit of the regulation in a methodical fashion. However, this document will not be prescriptive enough for organisations to use as a 'checklist'. The purpose for processing personal data, organisational risk appetite, and architectural decisions are some examples that require further consideration when formulating actionable projects.

Keeping with the principals of the regulation, this document focuses on:

- Providing techniques to uphold and maintain trust between data subjects, the organisation and regulators;
- Information on adopting mature information security practices to provide privacy;
- Providing an auditable process for third party validation 'doing the right thing'; and
- Allowing organisations to be agile on changes to the macro environment (social developments, regulation, technology).

The GDPR contains many elements presenting major challenges for organisations, breaking down the GDPR will provide organisations with a flexible approach to achieve compliance.

1.2. Document Considerations/Scope

While the GDPR is specific in its aim of protecting the privacy of people (data subjects), its reach is quite broad. As a result, the scope of this document is limited to cover important, common sections that affect most organisations that fall under the remit of the GDPR. This document outlines the governance for the GDPR as a project ensuring that the organisation establishes accountability while sub-projects ensure that specific GDPR requirements are met (Figure 1). Once the accountability requirements have been established, the operational requirements of the GDPR are managed by an existing privacy, legal or InfoSec team.

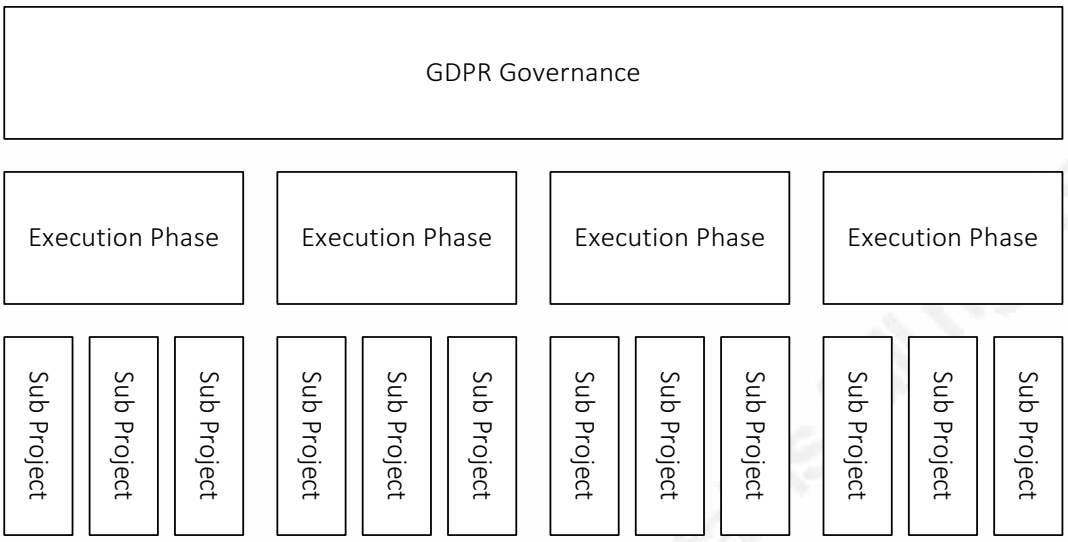

Figure 1: Relationship between Governance and sub-projects to achieve compliance with the GDPR

This document is designed to help organisations, data protection officers (DPOs) and information security professionals who are undertaking the GDPR compliance process. The focus is to allow organisations to lay a solid foundation to comply with the regulations and be able to adapt to impending legislative changes. The evolving nature of the GDPR means that information provided in this document is subject to variation due to EU Commission updates, case law, the output from the Article 29 Data Protection working party[1] and local Member State provisions or regional data protection authorities.

Organisations must be alert and agile to meet impending changes by understanding the concept of proportionality which is defined as the consideration of all available facts to determine a corrective course of action (SANS Institute, 2016). As the GDPR focuses on proportionality (Recital 4), organisations that adopt proportionality will remain agile and be in a strong position to maintain compliance with the GDPR (European Parliament, 2016; SANS Institute, 2016).

While strategic in nature, this document is laid out as a project for several reasons. Firstly, there is a set deadline for compliance where organisations must comply with the

[1] http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

GDPR by May 25, 2018 (European Commission, 2016). Using a project management framework provides the organisation with an end date for compliance.

Secondly, this document serves to provide governance over the organisation's GDPR implementation. Governance would provide outputs through sub-projects and operational processes. Splitting up the GDPR initiative into sub-projects has the benefit of producing achievable goals, maintaining clear objectives used for evidence of compliance, the ability to meet tight resource constraints, and to provide agility in line with future regulatory changes. Astute project managers will realise that this document is the abridged version of the PMI process groups and covers sections relating to most industries (PMI, n.d.).

Finally, a project management structure provides a starting point for organisations embarking on their GDPR initiatives. Using this document as a reference, organisations could consider points raised in this document when implementing their privacy management framework for the GDPR. The GDPR does not stipulate a specific privacy management framework, hence, organisations may choose an alternative framework such as BS 10012:2009[2] to aid with their compliance efforts. One benefit to adopting BS 10012 is the certification option attainable once the management framework is implemented, providing evidence that the organisation has taken action towards compliance (British Standards Institution, n.d.).

Where appropriate, guidance or recommendations will be suggested to aid in complying with the GDPR. Verification of compliance is crucial to keep in line with the regulation, with individual guidance providing auditable measures where possible. For the sake of generalisation, this paper will cover most sections within the GDPR except for cases such as "special categories" (eg: data relating to race, political opinions, beliefs, etc) (Article 9) and personal data relating to criminal convictions (Article 10) (European Parliament, 2016). Organisations will need to consider their individual situation on systems, projects, risk and resources to ensure the best fit for complying with the GDPR.

[2] http://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/

1.3. Non-EU Nations, Brexit, and the GDPR

Despite the GDPR being developed in Europe, global organisations seeking to expand their business must consider adopting practices stated within the GDPR to build trust amongst European citizens. Any organisation processing data on European Citizens are bound by the GDPR with severe penalties for violations. Despite not operating in the EU, organisations may leverage other means for US organisations seeking to process personal data regarding Europeans, such as Privacy Shield (Wright, 2016).

UK organisations currently processing the personal data of European citizens will need to align with the GDPR regardless of the implementation schedule for Brexit. With the UK Government confirming their support for the GDPR, organisations must align with the mandate (Denham, 2016). The UK Government and ICO will continue to engage in the process of negotiation to secure a deal with the EU Commission allowing the processing of citizen data (European Parliament, 2016). Depending on the outcome of negotiations, the UK may be within the scope of the GDPR or a 'third nation' as defined by the GDPR (Linklaters, n.d.; European Parliament, 2016). Once a deal has been reached, organisations will be in a good position to adjust their regulatory posture and comply with the final requirements. In doing so, organisations will be able to assure European customers that they have adopted governance aligned with the GDPR.

2. What is the GDPR and Its Objectives

The GDPR (EU Regulation 2016/679) serves to protect the right to privacy for individuals by holding organisations accountable for the safe processing of EU citizen personal data (Article 5) (European Parliament, 2016). Personal data is defined as data used to uniquely identify an individual (Recital 26) including digital data such as IP addresses (Recital 30) (European Parliament, 2016). In doing so, the regulation provides EU citizens greater control over their personal data handled by organisations. Some advantages for EU citizens include clear notification explaining the purpose of collecting personal data, ability to delete their personal information, ability to transfer between services and mandatory data breach notification.

The coverage of the GDPR makes it one of the widest reaching regulations in the world. Unlike other legislation which covers a specific industry (eg: GLBA, HIPAA), region (California's SB 1386), demographic (eg: COPPA) or sector (FISMA, FERPA), the GDPR encompasses all segments providing a level of uniformity for privacy (SANS Institute, 2016). The regulation affects organisations regardless of the industry and contains provisions for edge cases such as the handling of data relating to minors (Article 8) and criminal data (Article 10) (European Parliament, 2016). Organisations domiciled outside of the EU are also affected if the organisation processes data on EU citizens.

The GDPR also provides the foundation for the Digital Single Market, a strategy to leverage the use of technology to bolster economic growth across Europe (European Commission, 2016). Providing a privacy framework for organisations will serve to promote trust amongst citizens and help build confidence when purchasing online, thus benefiting organisations (European Commission, n.d.).

Similar to other industry-based regulations, such as SOX (SANS Institute, 2016), the focus for the GDPR is on self-regulation with compliance being evidence-based and verifiable. Transparency, accurate documentation, and vetting are crucial for compliance, providing evidence that organisations are respecting the rights of data subjects and information on processing. (SANS Institute, 2016).

As mentioned earlier, the GDPR is designed to be adaptive in nature, providing high-level guidance with the expectation of clarification through other instruments. While this flexibility causes confusion within organisations which must commit to the Regulation, it also allows environmental factors such as industry, society and technology to help shape the future of the Regulation (SC Magazine UK, 2016; European Parliament, 2016). Hence, organisations taking a strategic view through a culture of privacy as opposed to compliance will be able to adapt well to the evolving nature of the Regulation.

3. Initiating

Establishing governance is the first step towards complying with the GDPR through the implementation of governance as a project. Obtaining compliance with the GDPR is considered to be a project as it has a defined completion date (the GDPR

enforcement date), requires resources for implementation (staff, funds and materials) and, most importantly, there is a deliverable (compliance with the GDPR).

3.1. Project Charter

A project charter is required to justify the business requirement for complying with the GDPR through the initial establishment of governance and the approval to proceed with the project (SANS Institute, 2016). Justifications for the project should revolve around the following question, "What would happen to our organisation should a data breach expose personal information on our customers?" One strong justification sees this project as a mandatory legal requirement for organisations processing personal data on EU citizens. Hence, project success is defined as limiting exposure to liability resulting from noncompliance or a breach.

One of the inputs to the project charter is a statement of work (SOW) which is a set of work instructions articulating the tasks required for completion (SANS Institute, 2016). The strategic nature of the GDPR means that the SOW will need to provide deliverables which provide a long-term view for privacy and should include the following:

- The appointment of a Data Protection Officer to commence with the GDPR sub-projects.
- Installation of an assessable program to provide a cultural change towards privacy
- Implementation of a data identification program to identify existing and future data processing systems
- Maintenance of a record management system to keep track of data subject consent/requests, data processing, data protection impact assessments.
- Implementation of a process catering for data subject requests
- Development of a process to assess new systems for the protection of privacy
- Implementation and testing of an incident response system

Executed on an organisational level, the GDPR is a governance project which provides the necessary visibility and mandate required for success. Tasks from this project will be spawned off as sub-projects to address specific areas within the GDPR.

The project sponsor will need to be the CEO or at the very least a C-level executive, as this project may require a significant operational and cultural change across the organisation. Changes brought from this project will affect many departments, including the core business units such as sales, marketing, HR, finance, and IT. By examining the status quo through existing privacy policies, procedures and guidelines will help to determine the current privacy posture, the culture of the organisation, and the amount of change that is required to align with the GDPR (SANS Institute, 2016).

3.2. Stakeholders

Given that the GDPR affects the entire organisation, stakeholder support is critical to the success of this project. Compliance with the GDPR will require a significant amount of resources in order to comply before the enforcement date. As a result, senior management must accept ownership and sponsor the initiative. Explaining to stakeholders the organisational benefits that the GDPR can deliver will help garnish support.

Trust-based businesses would benefit from adopting the GDPR by reconfirming their commitment to privacy. A report commissioned by Symantec in 2015 discovered that European consumers see data security as the most important factor when choosing a company to do business with, rating higher than product quality and customer service (SC Magazine UK, 2016; Symantec, 2015). Consumers will be able to verify the organisation's commitment to GDPR through greater transparency on how the organisation will process consumer data.

Stakeholders will need to be aware of the penalties for infringement including a fine of up to €20 million or up to 4% of the total worldwide revenue for the organisation (Article 83) (European Parliament, 2016). The courts will consider several factors before issuing fines, applying penalties in proportion to the infringement (Article 83) (European

Parliament, 2016). These factors will take into consideration evidence of compliance taken by the organisation.

Establishment of governance requires the inclusion of the primary stakeholders. Primary stakeholders will need to understand the importance of the regulation, how it impacts the organisation and provide an undertaking to see that the organisation complies with the regulation as it comes into force. Stakeholders would include board-level executives, Information Security, IT and Legal departments. Board endorsement of the governance project sends a clear message to the organisation that compliance with the GDPR is an organisational-wide initiative. Also, the board will be able to provide material support such as budget allocation, approval for additional staff and organisation-wide directives.

Sub-projects will draw stakeholders from business units processing personal information and therefore, fall within the scope of the regulation. Business units include marketing, sales, support and customer research. Early engagement with the business units provides time for groups to identify data on EU citizens and earmark the necessary resources required to assist with compliance.

4. Planning

Complexities and time constraints of the GDPR require errors to be kept to a minimum as any rework would be costly. Meticulous planning to determine requirements for compliance, resources and project oversight is necessary to reduce mistakes and help to ensure a successful implementation of the GDPR.

4.1. Collect Requirements

Organisations seeking compliance with the GDPR will need to meet several objectives including, regulatory deadlines, incorporating measures to respect the rights and privacy of data subjects, and ensuring that personal information is processed securely. To achieve these objectives, organisations will need to determine requirements with respect to their line of business such as considering edge cases (SANS Institute, 2016). Some examples of edge cases include the processing of personal data relating to

children (Article 8), criminals (Article 11) and other sensitive data which protect an individual's "*rights and freedoms*" (Article 9) (European Parliament, 2016).

Organisational requirements will differ due to many factors such as industry and size, however, there are some requirements in some sub-projects that are common across organisations. Appointing a Data Protection Officer would be one such example, where the common requirement would be to employ a legal and security specialist to oversee the organisation's regulatory requirements.

4.2. Scope

The scope serves to define the outcome of the GDPR governance project (SANS Institute, 2016). From a governance level, the scope identifies the deliverables to be implemented through various sub-projects in order to establish a functional level for compliance. Governance affects all business units that deal with personal information, hence, the scope description would be similar to the following, "*This project will establish a level of governance to oversee that the requirements stipulated in the GDPR will be in place before May 2018.*" The deliverables of the governance project are based on the deliverables listed in the statement of work.

Sub-projects will have various scopes depending on the deliverable. As an example, the following criteria will require consideration when defining the scope for the data discovery phase, (European Parliament, 2016):

- Is there data in the organisation's possession that falls under the regulation?
- Was the data collected was done so in a legal manner? (Article 6-10)
- What is the type of data held on subjects? (Article 8-10)
- What are the geographical/legal jurisdictions in which the data will be processed? (Article 44-46)
- Will there be third parties involved with data processing? (Article 28, 29)
- Are there any edge cases that require further attention? (Article 9,10)

These questions may provide several deliverables such as creating records on data processing activities, implementing processes obtaining consent before future data collection, amendments to data transfer contracts with third parties, updating breach notification, and automated processing procedures.

4.3. Schedule

While the GDPR will come into force on May 25th, 2018, consideration must also be made for future provisions introduced by the Member States (European Parliament, 2016). Given the tight deadline, involvement is required from stakeholders to produce a plan for compliance by the deadline. Establishing governance for the GDPR must be completed as soon as possible to provide ample time to initiate sub-projects.

To reduce the time spent on sub-projects, 'quick wins' may be achieved through options such as decommissioning systems or processes handling personal data that may no longer applicable to the business, reviewing data retention periods, employing data security techniques such as encryption or tokenisation to reduce the potential exposure of personal information and the re-prioritisation of other data processing projects.

Other options to optimise meeting the requirements on time may be at the organisation's disposal once the later phases of the project are carried out. An example of optimisation would be to implement privacy awareness before the data audit stage, where privacy aware business units would proactively notify the DPO of systems processing personal data.

4.4. Costs

The GDPR uses the concept of proportionality to determine the effort required to secure personal data (Recital 83) (European Parliament, 2016). Keeping with the intent of the regulation, records outlining the decision-making process behind budgeting decisions would assist with the compliance process (SANS Institute, 2016). When determining the cost to comply with the regulation, organisations should ensure that legal representation is present to explore the options available for compliance (SANS Institute, 2016). The project must also consider proportionality as a balance between the costs of compliance

against the exposure to liability, considering the steep penalties associated with non-compliance.

Implementation costs vary due to a wide range of both internal and external variables such as the number of systems affected, the base currency used, local labour costs, and translations for communications (SANS Institute, 2016). As a result, organisations must consider their particular circumstances to determine the implementation costs for complying with the GDPR.

Governance of the compliance initiative will incur initial one-off costs. Some consideration for costs includes employing resources for the GDPR implementation projects, implementing a privacy education program, implementing systems for recording consent, and developing an incident response team.

Sub-project costs would include: employing project managers, auditing existing systems, developing processes to ensure new systems are designed with data protection in mind, and retrofitting controls to accommodate data subject requests. Ensuring that the cost of compliance is shared proportionally throughout the organisation, the governance team will assess and determine the costs associated with all sub-projects.

4.5. Human Resources Management

A project manager is required to oversee the implementation of governance. It is advised that a Data Protection Officer (DPO) assume the position of the project manager. Detailed information about the DPO is covered in the Execution phase. Additional resources required for fulfilling the requirements for governance would include internal communications, an incident response team and a public relations team. Extra resources may be needed to handle requests from data subjects depending on the size of the organisation, the handling process employed, and the level of automation employed within the organisation.

Project managers and technical, legal or business resources would be required to ensure that sub-projects would be completed at a professional level and before the enforcement of the GDPR. To meet the time constraints dictated by the GDPR,

organisations should consider the use of third parties or contract staff allowing sub-projects to operate in parallel.

4.6. Communications Management

Communications management is critical to the success of a project as complex as the GDPR. Miscommunication could result in lost time or information which could result in a substantial fine. As the project revolves around record management and attention to detail, capturing details serves as an important step in complying with the regulation. As a result, structured electronic communication would be a recommended medium.

With the introduction of governance, consolidated information could be presented to stakeholders. Status information from sub-projects can be relayed back to the governance team for tracking and reporting. Each sub-project would be reporting autonomously, only reporting as required by governance. Project status information could also be used for providing evidence of compliance.

Public communications must be published externally to ensure data subjects are informed of developments, promoting transparency between the organisation and the public. Publishing dates and change tracking of all public communication is critical to ensure that all parties are aware of new updates.

4.7. Risk Management

The controller (organisation) is bound by certain responsibilities such as the assessment of risks when processing data, as well as, providing adequate and proportional mitigations for those risks (Article 24) (European Parliament, 2016). The net effect of the GDPR could result in many changes within an organisation, introducing significant risk to business operations such as the disruption of services, shortage of skilled resources and the introduction of new security vulnerabilities. Governance serves to reduce risk across the organisation by splitting a monolithic project into smaller, manageable projects which will contain risks within specific projects.

Each organisation has different means and methodologies to deal with risks. As a result, the projects should adopt a risk management methodology which is approved by the organisation. Organisations could leverage risk management strategies adopted in

previous privacy based projects. One possible risk management strategy relating to data projects would include the identification of risks relating to the exposure or loss of data, consultation with subject matter experts or industry research on methods to limit data loss and formulating risk treatment plans for identified risks (reduce access to sensitive data, implement an authorisation process, etc) (SANS Institute, 2016). Projects involving personal data include data protection, business intelligence, and the implementation or migration of sensitive databases. Regulated organisations should consult strategies adopted in previous regulatory compliance/implementation projects (eg: GLBA, SOX). Finally, techniques such as consultation with stakeholders through brainstorming, Delphi technique, and interviewing would also aid risk management (SANS Institute, 2016).

When assessing risk, some factors for consideration include the impact on business for non-compliance, resources requirements, and environmental factors impacting on the project delivery (SANS Institute, 2016). Non-compliance issues include -regulatory fines, civil suits against the organisation, reputational damage, remediation costs. Issues relating to resource requirements include insufficient budget to achieve regulatory compliance, time constraints, lack of talent within the organisation. Environmental factors include supply chain issues for talent or materials (hardware or software), competing projects with higher organisational priority, potential loss of service when implementing sub-projects.

5. Executing

The bulk of the changes should occur during the execution phase. Each section below should be treated as an individual sub-project to be completed in the order in which they are listed below. Some functions will be projects on a governance level, while others will be implemented as sub-projects.

5.1. Establish a Data Protection Officer

The introduction of the GDPR raises the importance of a appointing a DPO within organisations. A Data Protection Officer (DPO) would assume the position of project manager for the governance of GDPR within the organisation, oversee the compliance initiative and be responsible for tasks listed in the regulation (Articles 37-39) (European

Parliament, 2016). Importantly, a DPO demonstrates to customers the organisation's commitment to upholding privacy, thus promoting trust.

While the GDPR currently states that employing a dedicated DPO is not mandatory, there are good reasons to have a dedicated DPO. With some Member States such as Germany adopting a "mandatory" requirement for a DPO, other Member States may decide to follow suit (juris GmbH, 2009; Linklaters, 2015). Having a dedicated DPO in anticipation of a mandatory requirement would potentially avoid talent shortages or salary increases as market demand increases. Furthermore, a dedicated DPO would keep abreast on the evolutionary nature of the GDPR and business operations by informing the organisation on how to remain agile within the regulatory environment.

A DPO requires a specific skill set to fulfil his or her duties. As part of Regulation 45/2001, the European Commission published professional standards[3] outlining details regarding the function of a DPO (European Commission, 2010). The DPO would be required to possess a legal, privacy and security background while expected to maintain independence from the organisation when performing his or her duties (Article 38) (European Parliament, 2016). Independence is akin to the role of an external auditor, ensuring that the DPO's duties do not result in a conflict of interest.

The professional standards for DPOs also outline best practices which are expected from DPOs, some of which align with several information security practices such as the implementation of data protection policies (Section 3.1), the implementation of data protection awareness programs (3.1), ensuring processes that uphold privacy (3.6), the investigation of incidents (3.7), continuous consultations with stakeholders on privacy related topics (3.5), maintaining a register of processing activities (3.3) and data subject requests (3.5) (European Commission, 2010). Implementation of these practices are sub-projects which will be discussed in later sections.

[3] http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf

5.2. Cultural Change Towards Privacy

An organisation's beliefs on privacy contrast consumer beliefs. A survey from Symantec discovered that organisations believed that their privacy track record was not a top consideration for customers while, customers rate their data security as the major factor when deciding which company to trade with (Symantec, 2016). This contrast in perception could lead to a decrease in sales with privacy dependent organisations incurring the greatest negative impact. This perception mismatch cannot be resolved solely through the implementation of the regulation, a culture of protecting EU citizen data throughout the organisation would help reduce the issue.

The DPO would oversee a governance level program to promote the importance of privacy amongst staff which would benefit the overall compliance efforts (European Commission, 2010). Having a privacy awareness program adopted at the governance level ensures that a consistently high level of awareness is maintained. Awareness programs include campaigns which are cyclical in nature helping to remind staff of their obligations for maintaining privacy and promote a cultural change towards privacy. To instil cultural change towards protecting privacy, the board must openly commit to promoting privacy, endorse privacy policies and champion awareness through education and training.

Promoting privacy through staff awareness is important to ensure that the organisation's privacy posture is consistent through the organisation. The main objectives of privacy awareness should at minimum include, reducing the number of privacy-related incidents through the promotion of good privacy practices and reducing the lead time with reporting a privacy incident.

5.3. Data Discovery

To effectively comply with the GDPR, the organisation must identify sensitive data about EU citizens which is achieved through a process of data discovery. The governance project will oversee the data discovery sub-projects ensuring that reasonable efforts have been made to discover and protect all personal data.

To help satisfy the GDPR reporting requirements, the data discovery project is comprised of three sequential phases: Data audit > Access control audit > Data Access audit. Once all phases are complete, records (detailed in a later section) are created outlining data stores, data flow and individuals with access to the data.

Data discovery revolves around one core question: *Has the department ever collected any data on individuals?* The question will help business units consider data that they collect and process. If any personal data is collected, then a record is required, regardless of any transformation of the data (eg: obfuscation, tokenisation or encryption).

The first step in the implementation of the data discovery project would be to identify high-level initiatives that would require the collection or protection of data such as operational requirements, best practices, industry compliance and regulation requirements. Business processes which use personal data provide insights into data flow, processing and access (Who is using the data, where is the data used, what is the data being used for?). Conditions associated with high-level initiatives such as the purpose for processing and retention periods provide key information for GDPR records.

Also, any prior data processing projects such as data categorisation would be of interest as it contains valuable information on the type and sensitivity of the data processed. Documentation of data flow completed by business intelligence projects would also greatly aid with data discovery as well as any Data Protection Impact Assessments (Article 35) (European Parliament, 2016). Example projects include database development (including big data and aggregation projects), business intelligence, data mapping and data loss detection/prevention eg: DLP, IDS/IPS.

Access control and data access audits will help identify users and the types of data accessed. This information enriches GDPR records with valuable information which could be used for accountability and breach investigations.

For completeness, other discovery techniques are available especially for organisations with decentralised IT teams or business units implementing unofficial IT solutions, colloquially known as ‘shadow IT’. These techniques include assessing departmental work processes and data flow, internal discovery (host/service/network) and

external discovery (cloud services, webmail, other services through software audits or network activity). Note that in some countries, the monitoring of employees may require HR, legal and work council approval (Norton Rose Fulbright, 2011).

5.4. Maintaining Records

The output from the data identification stage will aid with compiling records of data processing activities to satisfy Article 30 of the GDPR (European Parliament, 2016). The process of maintaining records is managed on a governance level ideally by the DPO. Derived from Article 30, records should contain the controller's details, the purpose of processing, categories associated with the processing of data, recipients of data, data transfers, retention strategy and related security measures (European Parliament, 2016):

Sub-projects should apply both technical and organisational security measures to protect data with respect to the requirements stated in Article 32 of the GDPR (European Parliament, 2016). The correct application of controls aligned with information security tenets such as the 'CIA triangle', availability, and auditing, is required to satisfy the regulation (European Parliament, 2016). Guidance can be obtained from standards such as ISO 27001, NIST SP800-53 (ISO, 2013; NIST, 2013).

Regular verification of the security controls is required as new threats, such as destruction, loss, unauthorised disclosure, affect data privacy (Article 32) (European Parliament, 2016). Despite the regulation not stipulating how to achieve verification, auditing through existing standards such as ISO 27001 provide a baseline in helping to achieve compliance. Organisations that handle sensitive data may be required to pursue further verification through extra measures including employee screening, active monitoring of log data and penetration testing. In the future, validation of the controls through certification (Article 42) could be obtained once the European Commission publishes approved certification bodies (European Parliament, 2016).

5.5. Respecting the Privacy of the Data Holder

Information about data processed regarding individuals will provide the organisation with an understanding of how to respect the privacy of individuals. The

GDPR specifies several areas which organisations are required to address such as obtaining consent, addressing data handling requests from the individuals. To address these areas, processes at a governance level are established to handle consent requests and organisation-wide communique such as the publication of data subject rights, service level agreements (SLAs) and so on. System specific modifications such as the user interface and the implementation of privacy controls will be implemented through sub-projects.

5.5.1. Consent

The GDPR requires consent for the collection of personal data by an organisation (Article 6-8) (European Parliament, 2016). The key concept behind consent is to ensure that requests for consent has been obtained and was done so in a clear and concise manner to reduce any potential misunderstanding. It is important that note that consent must be obtained in a legal manner (European Parliament, 2016). Legal consultation ensures that the organisation complies with the regulation's definition regarding consent. To address these concepts, consent is broken down into several elements.

Firstly, consent must be unambiguous meaning that the data subject must be presented with a clear statement explaining the organisation's use of their personal data before the subject taking some action expressing consent (Lee, 2016). In doing so, the subject would be aware of the reasons behind the collection of data as well as their rights. One example is a notice explaining the purpose behind collecting personal data on a web form.

For conditions of a more sensitive nature, explicit consent is required. Explicit consent is formal confirmation that the data subject agrees with the organisation's processing of the data's subject information. Explicit consent which may be achieved through a digital signature, an *unticked* checkbox on a website or oral statement (Recital 32) (European Parliament, 2016). Explicit consent is required for any processing of special data (Article 9), certain automated decision making (Article 22) or transfer of personal data (Article 49) (European Parliament, 2016). Conditions such as parental consent for processing children's data (Article 8) will require explicit consent from the children's parents (European Parliament, 2016).

The process of recording the subject's consent in a system is required as evidence and for auditing. Systems that could record this information include, but, is not limited to, databases (electronic consent), ticketing systems (oral based consent), document management systems (hardcopies, contracts, scanned copies) and traditional filing systems.

The data subject must be authenticated before the processing of any sensitive information. Authentication processes must be in place to ensure that the data subject made an authentic, legitimate request. In line with record keeping, authentication attempts should be recorded for future reference. While there is no official guidance on the regulation, controls from standards such as ISO 27001 (ISO, 2013) and NIST SP800-53 (NIST, 2013) would help the DPO prove that adequate measures have been taken to identify the data subject.

As data subjects have the right to withdraw consent (Article 7), organisations are required to cease processing data on the subject. A process will be required to handle the withdrawal of consent as well as the ability to record the progress of each request (European Parliament, 2016). A record will need to be created for proof of action and an acknowledgement sent to the data subject confirming the cessation of processing.

5.5.2. Data Subjects' Right to Their Data

The regulation provides more power to data subjects, giving them more rights over the data held by organisations. Data subjects have the right to access, correct, restrict processing, question the use of automated decision-making, delete (right to be forgotten), or transfer (data portability) their information (Articles 15-22), resulting in organisations having to track requests for compliance (European Parliament, 2016).

As stated in the GDPR, it is mandatory to inform data subjects of their rights (Article 15) (European Parliament, 2016). Part of this change would see privacy policies updated to reflect the changes brought about by the GDPR (White & Case, 2016). An external SLA is recommended to manage the processing expectations of data subjects assuring subjects that their rights are taken seriously. The SLA will need to be administered at a governance level, drafted in consultation with the respective stakeholders.

Data subject authentication is required before processing EU citizen data requests. Promoting staff awareness of data subject rights along with a process/system to track requests will help meet regulatory requirements (Article 12) and provides evidence for compliance (Article 39) (European Parliament, 2016). Business units must be aware of their obligations and process requests in a timely manner. Like the external SLA, an internal SLA could be implemented for business units to set time expectations for processing requests.

Honouring requests by data subjects to restrict processing requires the isolation of a record from processing. Recital 67 of the GDPR present methods where requests could be satisfied for simple instances. However, this approach may not be practical for complicated instances such as the processing of complex databases or fulfilling large numbers of requests (European Parliament, 2016). While the GDPR does not provide prescriptive examples for isolating records, it mentions that requests for restriction must be clearly indicated within the system (European Parliament, 2016). As a result, systems will require retrofitting with solutions such as flagging data, exception lists, or schema changes.

Satisfying the requirement to delete subject data is also a complicated task. Article 17 of the GDPR states some legal conditions processors must consider when assessing requests for deletion, such as, the validity of consent, rights of the subject that could overrule processing, and the necessitation to process data (European Parliament, 2016). As organisations have a legal right to obtain data for processing, organisations are required to assess deletion requests against these conditions with respect to their operations (White & Case, 2016). The assessment will decide whether to honour the request for deletion or provide an explanation as to why the request was denied (Article 19) (European Parliament, 2016). To ensure compliance with the GDPR, organisations must maintain a record of requests and their respective decisions.

Ed Yuwono, Ed.Yuwono.MSISM <at> gmail.com

The European Union Agency for Network and Information Security (ENISA) has published a guide[4] to help organisations satisfy requests for the deletion of personal data (ENISA, 2012). The guidelines cover several approaches depending on the type of system private (closed) or public (open) and propose various options to honour requests (ENISA, 2012). The regulation recognises the challenges with deleting information in the digital age and considers the principle of proportionality to determine if an organisation has taken reasonable steps to 'delete' data (Article 17) (European Parliament, 2016). To aid with compliance and the principle of proportionality, it is advised that organisations document deletion options that were explored and implemented.

The GDPR stipulates that service providers must provide data portability allowing data subjects with the possibility to migrate between providers (Article 20) (European Parliament, 2016). Many services such as social media, finance, and the government could benefit from data portability. Portability requires a common standard between service providers to simplify data transfer. While no official standard has been specified within the GDPR, service providers are required to collaborate on initiatives to satisfy this requirement. Initiatives such as the EU working group for Cloud Computing Contracts and the Data Portability Project may help organisations fulfil data portability requirements (European Commission, 2016; Data Portability Project, n.d.). However, the success of data portability requires trust between providers. Intervention and support from governing bodies is required to facilitate trust and provide a platform for collaboration. Initiatives such as the EU Digital Single Market, UK Government's *midata* and the Dutch *Zeker-Online* programs will help progress plans for a future for data portability (European Commission, n.d.; UK Government, 2011; Zeker Online, n.d.).

5.5.3. Automated Processing

Technology is used to provide decisions such as assessing an individual's eligibility for a home loan or when calculating insurance premiums. In some instances, automated decision making could have a detrimental effect on an individual. Under the

[4] https://www.enisa.europa.eu/publications/the-right-to-be-forgotten/at_download/fullReport

GDPR, an individual has the right to query or prevent the use of any automated decision making process (Article 21, 22) requiring organisations to establish suitable processes for each situation (European Parliament, 2016).

The data subject must be made aware of any automated system used to evaluate a person's status (Article 13) (European Parliament, 2016). Systems must be modified to provide the data subject details of any automated processing. Informing the data subject of automated processing would best be done at time of consent.

An individual can opt out of any automated systems which process their personal data (Article 19) (European Parliament, 2016). Should an individual elect not to use a system, alternatives such as manual processing or complete cessation of processing must be available to the user. An example of this would be an individual requesting a loan and making sure that the individual has the option for the bank to assess the application through non-automated means.

If a decision is made through an automated system, a data subject could request information on how their situation was assessed and the expected result (Article 14) (European Parliament, 2016). For example, if a system was used to assess an individual's credit application, a data subject may request to know how their data will be used and what the potential outcome would be.

It is important to note that when automated systems are used, suitable measures must be in place to respect the data subject's rights (Recital 71) (European Parliament, 2016). Generally speaking, the data subject has the right to question or appeal a decision made by an automated system. One example is when a data subject's loan application is rejected, they would have the right for a loan officer to review their case.

5.5.4. Transfer of Data to Third Parties

Data collected from subjects are subject to limitations for processing including, restrictions on where data can be transferred (Article 44) and who is permitted to process data (Article 28, 29) (European Parliament, 2016). Subsidiaries of multinational organisations or organisations outside of the EU that process data on EU citizens are required to adhere to the regulation (Article 44) (European Parliament, 2016). Prior to

transfer, entities are assessed against criteria including the rule of law (Article 45), employing appropriate safeguards for protecting data (Article 46) and corporate rules (Article 47) (European Parliament, 2016). Transfer of personal data to a third party or outside of the EU requires explicit consent from the individual (European Parliament, 2016).

Organisations that seek to transfer data to a third party (processors) for processing will need to ensure that the processor provides sufficient guarantees that data subject privacy is maintained (Article 28) (European Parliament, 2016). Legal responsibilities between the organisation and the processor are transitive, meaning that, both organisations share the liability resulting from personal data incidents (European Parliament, 2016). The onus is on the organisation to provide the processor with clear instructions on how to handle personal data (Article 29) (European Parliament, 2016). This responsibility is particularly important for organisations that utilise service providers such as cloud or *aaS providers.

While the restrictions on the transfer of citizen data outside of the EU is not new, the restrictions have been upheld within the GDPR (SANS Institute, 2016). To legally transfer data outside of the EU, several instruments could be used such as commission rulings, legal contracts, administrative and technical controls (Articles 45-47) (European Parliament, 2016).

Although many nations outside of the EU have data protection regulations, these regulations may contain variations making them incompatible with the GDPR (DLA Piper, 2016). The European Commission compiled a list of nations that are deemed "adequate for transfer" (Article 45), meaning that the legal stance on privacy within these nations are sufficient enough to meet the conditions of the GDPR (IAPP, 2016; European Parliament, 2016). Separate agreements permitting transfer have been drafted between other nations that do not have compatible privacy laws, such as Privacy Shield between the EU and the US (European Commission, 2016).

Until such time that an agreement can be reached with other nations (Article 50), contractual agreements between organisations must be in place to ensure that data protection laws are respected (Article 47) (European Parliament, 2016). These

agreements must ensure that the organisation outside of the EU adheres to an equivalent data protection standard meeting the concepts listed in the GDPR (IAPP, 2016).

5.6. Breach Notification

In the event of a breach, the GDPR contains a requirement where the organisation must provide notification to the DPO or the supervisory authority within 72 hours (Article 33, 34) (European Parliament, 2016). While breach notification in incident handling is not new, the GDPR defines this as a legal requirement (Article 33) (European Parliament, 2016).

For organisations to comply with the regulation, certain information must be provided as part of the notification (Article 33, 34) (European Parliament, 2016). A pre-established incident response team aware of the organisation's obligation to breach reporting will be able to convey the necessary information to the DPO. The governance project will be required to inform incident response teams on the requirements and of any new developments on the GDPR.

Completing earlier phases such as data discovery will provide incident handlers with an excellent starting point for determining if a data breach has occurred. Knowing the type and location of data being processed will help incident handlers determine if any sensitive data has been compromised (Buffington, 2008). With the DPO's involvement, the DPO could consult with the board, legal and public relations teams with formulating a communication plan to the supervisory body or data subjects.

Given the GDPR's requirement to report within 72 hours, employees must be aware of their roles during an incident (European Parliament, 2016). Awareness can be achieved through education and experience gained through incident response drills. Records of awareness programs and drills should be maintained as regulatory evidence. Frequency, drill results and post-mortem information provides information for measuring changes to organisational culture.

Several standards are available that would help organisations establish and operate an Incident Response team such as the Computer Security Incident Handling

Guide by NIST or ISO/IEC 27035:2011 Information security incident management guide (NIST, 2012; ISO, 2011).

Article 33 stipulates that documentation regarding a breach will need to be presented to the supervisory body (European Parliament, 2016). As a result, it is critical that the incident notes and post-mortem documentation contain details of the event and the remediation steps to allow a third party to assess the breach.

Finally, it is important to note that notification is not required if the breach relates only to encrypted data (Article 34) or if the breach does not impact on the rights of individuals (Article 33) (European Parliament, 2016).

6. Closing Process

The closing process involves the handover of ongoing tasks to operational teams. The two sections below outline processes required for design teams and operational teams respectively. The DPO would oversee that these two processes are carried out beyond the adoption of the GDPR within the organisation.

6.1. System Design

The GDPR recognises that designing systems with privacy in mind will serve to reduce the risk of a data breach (Article 25) (European Parliament, 2016). While the regulation does not provide specific guidance, data retention, data minimisation and pseudonymisation strategies would serve to align with the regulation (European Parliament, 2016).

If the organisation believes that processing would have an adverse impact on data subjects, a Data Protection Impact Assessment (DPIA) must be performed before the processing of personal data (Article 35) (European Parliament, 2016). To provide evidence of due diligence, it is recommended that all existing systems processing personal data undergo a DPIA. In consultation with stakeholders, the governance project would maintain standards for the DPIA and maintain the associated records.

The DPIA process is designed to assess a system's ability to maintain the privacy of individuals (European Parliament, 2016). The principle of secure by design can be

proven by conducting a DPIA during the design stage which could identify design deficiencies and improve the system design process (European Parliament, 2016). The system architect would be required to consult with the DPO to help ensure that all privacy concerns raised in the DPIA are addressed. In the event where the result of a DPIA classifies a system to be high risk, the DPO will need to consult with the supervisory authority for further advice (European Parliament, 2016).

While the GDPR does not specify a particular standard to conducting a DPIA, the UK Information Commissioners Office has released a guide[5] on conducting a Privacy Impact Assessment (PIA) which outlines several areas for consideration with respect to the Data Protection Act (UK Information Commissioner's Office, 2014). As a result, modifications to the PIA may be required to accommodate requirements from the GDPR.

The design process will need to balance the needs of the organisation and the privacy of the individual. With this in mind, ENISA has explored the concept of privacy by design and provided eight high-level strategies by combining legal and technical strategies: minimise, hide, separate, aggregate, inform, control, enforce, demonstrate (ENISA, 2015). Appropriate strategies could be employed for each phase of processing within the organisation (ENISA, 2015).

While it is voluntary, verification of system design could also be achieved through independent audits or certification (Article 42) (European Parliament, 2016). The European Commission is expected to publish a list of approved certification bodies sometime in the future (European Parliament, 2016).

In organisations with a laissez-faire approach to design, organisational policies, staff awareness and education will be required to limit the presence of ‘shadow IT’ preventing undocumented systems from processing personal data.

Finally, records detailing information on new systems must be kept with the DPO (Article 30) (European Parliament, 2016).

[5] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

6.2. Ongoing Compliance with the GDPR

The governance team should oversee operational teams ensuring that compliance with the GDPR is maintained. While some of the tasks assigned to the governance team have been addressed in other sections as sub-projects, other tasks would be transitioned to operational processes. For example, the governance team will be expected to maintain a register of data subject requests as evidence proving that the organisation is handling requests in a timely manner.

Over time as the GDPR reaches a level of maturity, further changes such as local adoption of the regulation are expected, requiring organisations to adjust accordingly. Regular consultation with the governance team and stakeholders will be required to ensure compliance with new developments. Organisations must also be aware that there may be occasions where the local supervisory authority may request information regarding their compliance initiatives (Article 31) (European Parliament, 2016).

An organisation could leverage GDPR records as inputs for strategic initiatives. One example would be to determine if encryption cyphers within the organisation are no longer fit for use. Organisations can decide on what decisions have previously been made to replace old cyphers, the systems affected, and to produce a plan for replacement.

7. Conclusion

With the deadline approaching, the GDPR will require organisations to prioritise current operations to achieve compliance. While there are a lot of unanswered questions concerning sections within the GDPR, organisations that have implemented key privacy measures will be able to adapt better to future developments in the regulation.

Implementing a strong level of governance for the GDPR demonstrates a level of commitment and provides stakeholders with the ability to monitor the progress for compliance. The strategies presented throughout this document will hopefully serve others by promoting constructive and innovative solutions for achieving compliance.

References

British Standards Institution. (n.d.). *BS 10012 Personal Information Management System* . Retrieved from British Standards Institution: http://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/

Buffington, J. (2008). *Breach Notification in Incident Handling.* Retrieved from SANS Reading Room: https://www.sans.org/reading-room/whitepapers/incident/breach-notification-incident-handling-2114

Burkert, H. (2000). Privacy-Data Protection. *Governance of Global Networks in the Light of Different Local Values*, 43-70.

Centre for Information Policy Leadership. (2016, May 6). *Workshop Report - Implementing and and Interpreting the GDPR: Challenges and Opportunities.* Retrieved from Centre for Information Policy Leadership: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_amsterdam_workshop_report.pdf

Data Portability Project. (n.d.). *Data Portability Project*. Retrieved from Data Portability Project: http://dataportability.org/

Denham, E. (2016, October 31). *How the ICO will be supporting the implementation of the GDPR.* Retrieved from UK Information Commissioner's Office blog: https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/

Deutsche Welle. (2011, January 26). *France maintains long tradition of data protection*. Retrieved from DW: http://www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711

DLA Piper. (2016). *Data Protection Laws of the World.* Retrieved from Global Data Protection Handbook: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all

ECHR. (2010, June 1). *European Convention on Human Rights*. Retrieved from European Court of Human Rights: http://www.echr.coe.int/Documents/Convention_ENG.pdf

ENISA. (2012, November 20). *The right to be forgotten - between expectations and practice.* Retrieved from ENISA: https://www.enisa.europa.eu/publications/the-right-to-be-forgotten/at_download/fullReport

ENISA. (2015, December). *Privacy by design in big data - Enisa - Europa.* Retrieved from ENISA: https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport

European Commission. (2010, October 14). *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001.* Retrieved from European Commission: http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf

European Commission. (2014). *Switching - Data portability upon switching*. Retrieved from European Commission: http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_topic_4_switching_en.pdf

Ed Yuwono, Ed.Yuwono.MSISM <at> gmail.com

European Commission. (2016, September 29). *Commission decisions on the adequacy of the protection of personal data in third countries*. Retrieved from European Commission: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

European Commission. (2016, September 29). *Expert Group on Cloud Computing Contracts*. Retrieved from European Commission: http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm

European Commission. (2016, September 29). *Reform of EU data protection rules*. Retrieved from European Commission: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

European Commission. (n.d.). *Digital Single Market*. Retrieved from European Commission: https://ec.europa.eu/priorities/digital-single-market_en

European Parliament. (1995, November 23). *Directive 95/46/EC of the European Parliament and of the Council*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN

European Parliament. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

IAPP. (2016, January 19). *Top 10 operational impacts of the GDPR: Part 4 - Cross-border data transfers*. Retrieved from IAPP: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/

ISO. (2011). *Information security incident management ISO/IEC 27035:2011.* Retrieved from ISO: https://www.iso.org/obp/ui/?_escaped_fragment_=iso:std:44379:en#!iso:std:44379:en

ISO. (2013, September 25). *ISO/IEC 27001:2013.* Retrieved from ISO: http://www.iso.org/iso/catalogue_detail?csnumber=54534

juris GmbH. (2009). *German Data Protection Act (BDSG).* Retrieved from Gesetze im Internet (Laws on the Internet): https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

Lee, P. (2016, June 7). *The ambiguity of unambiguous consent under the GDPR*. Retrieved from Privacy Law Blog - Fieldfisher: http://privacylawblog.fieldfisher.com/2016/the-ambiguity-of-unambiguous-consent-under-the-gdpr/

Linklaters. (2015, July). *Data Protected Report.* Retrieved from Data Protected: https://clientsites.linklaters.com/Clients/dataprotected/Pages/index.aspx

Linklaters. (n.d.). *The GDPR at a glance, and a "to do" list to help you prepare for it*. Retrieved from Linklaters: http://www.linklaters.com/pdfs/mkt/london/General_Data%20Protection_Regulation_GDPR_Brochure_WEB_FINAL_Spreads3.pdf

Newman, A. L. (2008). Building transnational civil liberties: Transgovernmental entrepreneurs and the European Data Privacy Directive. *International Organization, 62(01),* , 103-130.

Ed Yuwono, Ed.Yuwono.MSISM <at> gmail.com

NIST. (2012, August). *Computer Security Incident Handling Guide SP 800-61 rev 2.* Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST. (2013, January 22). *Security and Privacy Controls for Federal Information Systems and Organizations.* Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Norton Rose Fulbright. (2011, December). *Global Update: Monitoring your employees' use of technology | Australia | Norton Rose Fulbright*. Retrieved from Norton Rose Fulbright: http://www.nortonrosefulbright.com/knowledge/publications/60434/global-update-monitoring-your-employees-use-of-technology

PMI. (n.d.). *PMBOK® Guide and Standards.* Retrieved from PMI: https://www.pmi.org/pmbok-guide-standards

Privacy International. (n.d.). *What is Privacy*. Retrieved from Privacy International: https://www.privacyinternational.org/node/54

SANS. (2016, September 16). *Incident Handling White Papers.* Retrieved from SANS: https://www.sans.org/reading-room/whitepapers/incident

SANS Institute. (2016). *LEG523: Law of Data Security and Investigations.* SANS Institute.

SANS Institute. (2016). *MGT525: IT Project Management, Effective Communication, and PMP® Exam Prep.* SANS Institute.

SC Magazine UK. (2016, October 18). *EU GDPR - nine out of ten don't understand it*. Retrieved from SC Magazine UK: http://www.scmagazineuk.com/eu-gdpr--nine-out-of-ten-dont-understand-it/article/561793/

Symantec. (2015). *State of Privacy Report 2015.* Retrieved from Symantec: http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

Symantec. (2016, October). *Symantec State of European Data Privacy 2016.* Retrieved from Slideshare: http://www.slideshare.net/symantec/symantec-state-of-european-data-privacy

UK Government. (2011, November 3). *The midata vision of consumer empowerment*. Retrieved from UK Government: https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment

UK Information Commissioner's Office. (2014, February 25). *Guide to data protection.* Retrieved from UK Information Commissioner's Office: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

White & Case. (2016, July 22). *Chapter 9: Rights of data subjects – Unlocking the EU General Data Protection Regulation*. Retrieved from White & Case: http://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation

Wright, B. (2016). STI Professional Lecture Series: Turmoil in European Data Privacy Law. US.

Zeker Online. (n.d.). *Zeker Online*. Retrieved from Zeker Online: https://www.zeker-online.nl/

Ed Yuwono, Ed.Yuwono.MSISM <at> gmail.com