EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Challenges of Complying with Data Protection and Privacy Regulations

A.M. Lonzetta, T. Hayajneh*

Fordham Center for Cybersecurity, Fordham University, New York, NY 10023, USA

Abstract

As we move into a more digitized society, the collection and use of data continues to increase. This influx in data, partnered with challenges complying with data protection and privacy regulations and the absence of a comprehensive global data protection and privacy strategy, has contributed to data breaches and data misusage. In order to reduce these incidents, updates must be made to existing regulations and included in future regulations. A global agency should also be created to identify the main data protection and privacy objectives to develop a comprehensive strategy and oversee data protection and privacy. Our paper presents an overview of existing data protection and privacy regulations, the challenges of complying with the regulations, and recommendations to achieve long-term data protect and privacy.

Keywords: GDPR, CCPA, Data Privacy, Data Protection Regulations, Compliance

Received on 20 May 2020, accepted on 09 September 2020, published on 18 September 2020.

doi: 10.4108/_____

1. Introduction

There are currently hundreds of laws related to privacy dating back to colonial America, including criminal law, the common law of torts, constitutional law, evidentiary privileges, federal statues, and state statues [1]. In the beginning, the primary purpose for the enactment of these laws was to ensure citizen's freedom from government institutions [1].

In the last decade of the twentieth century, the introduction of internet technology has posed new, challenging threats [1]. Internet technology has become an essential part of peoples everyday lives. It includes the use of email, online shopping, online searching, social media, etc.. Its usage has resulted in the generation of a significant amount of personal data that is collected, used, shared, stored, and sold by organizations, governments, and third parties (e.g. data brokers) [2,3].

Organizations utilize the collected data to develop a more strategic approach to common business initiatives, including product development, product solutions, consumer targeting, consumer experience, optimization of operations and supply chains, and the identification of future market trends [4]. Data is used by governments and law enforcement for identification for arrest warrants, as well as physical and digital surveillance. In both organization and government instances, data is used to create personal profiles, some of which are used to influence behaviour.

Individuals are becoming more aware of personal data collection and usage. A recent U.S. study found that the majority of Americans are concerned about how their personal data is being used [5]. Figure 1 below shows that there are significantly more individuals concerned about how companies and the government use personal data compared to those who are not [5]. It also shows that individuals are most concerned about the use of their personal data by companies [5].

*Corresponding author. Email: Dr.thaier@gmail.com

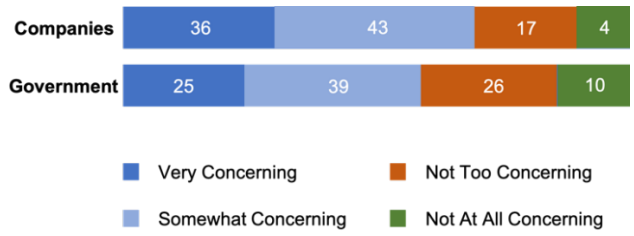

Figure 1. Data Usage Concerns

The necessary steps must be taken to protect personal data. This includes how the data is collected, processed, shared, and stored.

The objectives of this paper are:

A. Present an overview of data protection and privacy regulations, with a focus on their scope and objectives

B. Identify the challenges of complying with data protection and privacy regulations

C. Discuss several recommendations that will assist in achieving data protection and privacy in the long-term.

The remainder of this paper is organized as follows. Section 2 presents related work. Data protection and privacy regulations are discussed in Section 3. Section 4 discusses challenges of data protection and privacy regulation compliance. Section 5 provides recommendations for mitigating challenges related to data protection and privacy regulation compliance and achieving data protection and privacy in the long-term. Finally, Section 6 provides a conclusion for the paper.

2. Related Work

As the collection and usage of personal data increases, privacy and data protection experts continue to conduct research and work with lawmakers to protect personal data.

In "Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)", the authors examine the challenges organizations face when trying to comply with GDPR [6]. The study was published shortly after the enforcement of GDPR and only a select number of candidates were interviewed. As more organizations continue to provide feedback on GDPR, more challenges have been identified. This is further discussed in our work.

In "GDPR Compliance in Norwegian Companies", the authors conducted an online survey which identified and described opportunities and challenges faced by Norwegian companies when trying to comply with GDPR [7]. We explore these challenges further, and identify those and others that are encountered when trying to comply with data protection and privacy regulations.

The majority of research on this topic focuses on GDPR, with minimal to no research done on other regulations. Additional research has been conducted and papers have been published; however, they extend beyond the focus of our work.

3. Data Protection Regulations

In this section, we discuss the various global data protection and privacy regulations. They are divided into three categories - early data protection and privacy regulations, recent data protection and privacy regulations, and upcoming data protection and privacy regulations.

3.1. Early Data Protection and Privacy Regulations

The regulations listed below are some of the earliest data protection and privacy regulations passed [8].

The Privacy Act of 1988

The Australian Privacy Act of 1988 is the primary privacy regulation in Australia [8]. Over the years, it has gone through two sets of amendments. The first in 2000, which expanded the regulation to cover private sector businesses. The second and more comprehensive update was done by the Australian Law Reform Commission in 2014.

The main objective of the regulation is to enable information to flow freely outside of Australia, while respecting individual privacy in relation to information collection, use, disclosure, disposal, access, integrity, and credit reporting. The regulation applies to Australia, Australia Capital Territory, Norfolk Island government agencies, and private businesses. Organizations with less than $3 million in annual sales do not need to comply with the regulation. The regulation consists of 13 principles which are detailed below.

Openness and Transparency in the Management of Personal Information. All information should be managed openly and transparently. Entities are required to have a privacy policy that is clear and addresses specific matters [8]. The necessary steps should be taken to comply with The Privacy Act of 1988.

Anonymity and Pseudonymity of Information. Individuals should have the opportunity, unless exempt, to not be identified.

Collecting Solicited Information. Personal information should be collected by "lawful and fair means". It should only be collected when it is necessary or associated with the entity's function or activities. Consent is needed to collect sensitive information.

Handling Unsolicited Personal Information. Unsolicited information must be anonymized or destroyed [8]. This includes information that could not have been collected under the previous principle.

Notification for the Collection of Personal Information Individuals must be notified when personal information is collected.

Disclosure or Use of Personal Information. Information collected for a specific purpose must be used for that purpose. In order to use it for other purposes, the entity needs the individual's consent. Matters related to law enforcement, as well as health and safety are exempt.

Personal Information for Direct Marketing. Personal information used for direct marketing requires the use of an opt-out for future messages. Sensitive information on individuals requires consent for direct marketing.

Overseas Disclosure of Personal Information. Overseas recipients of personal information must adhere to the Australian Privacy Act. Information should only be disclosed to recipients when they adhere to similar regulations, consent is received, or there is an exception. This must be confirmed before the disclosure of the information. In the case recipients do not adhere to the regulations, the entity could be liable.

Use, Disclosure, or Adoption of Government Related Identifiers. Government related identifiers for individuals cannot be adopted by entities to use as their own. They also cannot use or disclose this government related identifier unless there is an exception.

Personal Information Quality. Personal information collected, used, or disclosed must be accurate, up-to-date, and complete.

Security of Personal Information. Personal information must be protected from misuse, unauthorized access, interference and loss, disclosure, and modification. Information that is no longer required for business reasons should be anonymized or destroyed.

Access to Personal Information. Individuals must have access to their personal information.

Personal Information Correction. In the case that individuals request corrections to their personal information, steps must be taken by the entities to make these corrections.

Privacy Act of 1993

The primary purpose of New Zealand's Privacy Act of 1993 is to protect individuals [9]. It addresses the collection, use, and storage of identifiable personal data which effects consumer marketing [9]. This regulation was used as a framework by other countries for their privacy regulations [9]. It is comprised of 12 principles which are detailed below [10].

Purpose of Personal Information Collection. There must be a lawful purpose that aligns with the organization's mission for personal data collection. Collection of personal data must be necessary to fulfill that purpose.

Source of Personal Information. Information collected must be obtained directly from the individual, except in the case that the information is public.

Collection of Information from the Subject. Organizations must notify individuals about information collection, the reason for the collection, who the information will be shared with, the name and location of the agencies that collect and manage the information, regulations related to the authorization of the collection, whether the collection was voluntary or mandatory, and the results of not providing requested information.

Manner of Collection of Personal Information. Data collection cannot be unlawful, unfair, or intrusive. Transparency is required.

Storage and Security of Personal Data. Stored data must be secured to prevent loss, access, use, modification, unauthorized disclosure, or misuse.

Access to Personal Information. Individuals can request confirmation on whether the agency has their information. They are also entitled to access that information.

Correction of Personal Information. Individuals can request corrections to their information and the agency must make reasonable changes.

Accuracy of Personal Information to be Checked Before Use. Agencies must ensure personal information is accurate, up-to-date, complete, relevant, and not misleading.

Agencies Must Not Keep Personal Information Longer than Necessary. Agencies should not retain information longer than needed to fulfill the purpose for which it was collected.

Limits on Use of Personal Information. Agencies that collect information must use it for purposes originally stated, unless a reasonable exception applies. Exceptions include information that is public, is authorized by the individual, would not cause prejudice, is necessary to reduce a threat, is used for a purpose related to that in which it was originally obtained, or is anatomized.

Limits on Disclosure of Personal Information. Agencies cannot disclose personal information unless it is related to the purpose in which it was collected, the information is public, the individual authorizes the disclosure of the information, the information would not prejudice the individual, the information is necessary to reduce a threat, the information is necessary for the sale of a business, or the information is anatomized.

Unique Identifiers. Unique identifiers should not be assigned to information. Exceptions include identifiers that increase efficiency of an organization or for the disclosure in which the identifier was assigned.

Data Protection Directive (Directive 95/46/EC)

The EU Data Protection Directive, also known as the Directive 95/46/EC, was adopted by the European Union in 1995 to protect the privacy and personal data of EU citizens [11]. It is comprised of 7 principles which are detailed below.

1. Individuals should be given notice when their data is collected.

2. Individuals should be informed of the party or parties collecting their data.

3. All personal data collected should be safeguarded from abuse, theft, or loss.

4. Consent is needed from data subjects to disclose or share data with third parties.

5. Individuals should have access to their personal data, as well as the ability to correct any inaccuracies.

6. Data collected should only be used for purposes stated when it was originally collected. It should not be used for any other purposes.

7. Data subjects must be able to hold personal data collectors accountable to all principles outlined.

Personal Data (Privacy) Ordinance

Hong Kong's Personal Data (Privacy) Ordinance was passed in 1996 [12]. Its primary purpose is to protect personal data [12]. In 2012, an Amendment Bill expanding the scope to include the use of personal data for marketing purposes was passed [12]. The ordinance is comprised of 6 principles which are detailed below.

Data Collection Principle. The collection of data must be done in a lawful and fair manner [12]. Data should only be collected if it is being used [12]. Data subjects must be aware of the purpose for collection and usage, as well as third parties who may receive the data [12].

Accuracy & Retention Principle. The organization should take the necessary steps to ensure personal data is accurate. Data should only be kept as long as it fulfills its purpose.

Data Use Principle. The use of personal data is limited to the purpose in which it was collected or related purposes. In the case voluntary or explicit consent is given, there is an exception.

Data Security Principle. Practical steps to safeguard data from unauthorized access, accidental access, unauthorized processing, erasure, loss, or unauthorized use must be taken.

Openness Principle. Steps must be taken to make individuals aware of data policies, practices, and usage.

Data Access & Correction Principle. Individuals must be given access to their personal data and have the ability to make corrections when data is inaccurate.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The United States' Health Insurance Portability and Accountability Act of 1996 protects a patient's health information. This information is also known as "protected health information" [13]. It aims to prevent disclosure of protected health information without a patient's knowledge, consent, or authorization, while still enabling the flow of health information to promote and maintain quality healthcare and protect public health [13]. The regulation applies to healthcare providers, health plans, healthcare clearinghouses, and business associates [13]. The entities must:

1. Protect the confidentiality, integrity, and availability of healthcare information.

2. Safeguard healthcare information from security threats. Entities must take the necessary steps to detect these threats.

3. Protect health information against foreseen prohibited use or disclosure.

4. Certify workforce compliance.

Data Protection Act 1998

The UK was encouraged after the passing of the EU Data Protection Directive [14]. In 1998 they went on to pass the Data Protection Act to protect citizen's rights related to personal data collection and protection [14]. It is comprised of 8 principles which are detailed below [14].

Fair and Lawful Use. Organizations need to be transparent when it comes to collecting and using data. There must be transparency around the identity of the data controller.

Clear Purpose. The reason for collecting data must be clear and conveyed to the data subject. Data should only be used for purposes originally stated. In the case it will be used for other purposes, additional consent is needed and the purposes must be disclosed.

Adequacy, Relevancy, and Reasonable Use. Organizations should not collect information in excess of what is needed for purposes originally stated.

Accuracy of Information. Information on the data must be accurate, including the origin and meaning. All data must be kept up to date.

Storage and Retention. Data should not be kept longer than needed to fulfill the purposes originally stated.

Individual Rights. Individuals have the right to access their information and decline the use of any data that would be damaging or distressful. Individuals have the ability to refuse the use of their data for marketing or automated purposes. They have the right to ensure the accuracy of their data and request its deletion if it is incorrect.

Security. The proper safeguards should be put in place for the collection, storage, and disposal of data to prevent unlawful use or accidental loss.

International Use. Data can only be transferred to nations that have similar or higher safeguards for personal data processing.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act, also known as the Financial Modernization Act of 1999, repealed previous laws targeting financial institutions. It also mandated additional privacy protections for financial institutions that service customers [15]. It aims to protect nonpublic personal information, which includes personal information provided for financial products or services, transaction information, and information obtained from consumer reports or court

records [15]. Below are the key items set forth in the law [16].

1. The appropriate administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer data must be put in place. Data must also be protected from unauthorized access. Consumers must be notified of the safeguards that are put in place [15].

2. Financial institutions must provide notice to consumers about the type of nonpublic information collected and how it is used.

3. Individuals must be able to opt-out of financial institutions sharing nonpublic information with specific third parties. Financial institutions should not disclose account number information for marketing purposes.

4. When establishing customer relationships, financial institutions must disclose its privacy policy. It must include categories of nonpublic information that is collected, policies and practices of the institution, and the categories of information that may be disclosed.

5. Information from consumers must not be received under false pretenses. Financial institutions that knowingly or intentionally violate this section could face criminal penalties.

6. The regulation must be enforced.

Personal Information Protection and Electronic Documents Act

Canada's Personal Information Protection and Electronic Documents Act went into effect in 2000. Its primary purpose is to build trust in electronic commerce by governing the collection, use, and disclosure of personal information. It has since expanded to additional industries, including banking, broadcasting, and healthcare [17]. All private sector organizations must adhere to the regulation. It is comprised of 10 principles which are detailed below [18].

Accountability. All information held by the organization should be protected. Policies and practices surrounding personal information should be developed and implemented. All relevant organizations should comply with the principles of the regulation. Someone should be appointed to be responsible for compliance.

Identifying Purposes. Organizations need to understand the purpose for which they are collecting information to ensure they are only collecting data that is needed. Individuals must be notified about why their information needs to be collected.

Consent. Meaningful consent is needed from individuals to use, collect, or share their information. Individuals need to understand what they are consenting to and the consequences of providing consent. Consent can only be required when the information is necessary. Individuals can withdrawal their consent at any time, but they must be informed of the implications this will have [18].

Limiting Collection. Only information that has a specific purpose should be collected. Honesty about the reason the data is being collected is necessary and all information must be collected fairly and lawfully.

Limiting Use, Disclosure, and Retention. Data can only be used or disclosed for purposes identified when it was collected. Information can only be kept long enough to serve the purposes for which it was collected. Organizations must understand what data they have and how it is being used. Consent is needed if data will be used or shared in ways not previously identified. Data must be used appropriately. Organizations must have guidelines in place for the retention and destruction of data. Information no longer needed must be destroyed or anatomized.

Accuracy. Accurate information must be kept and used.

Safeguards. Information must be safeguarded from loss, theft, unauthorized access, disclosure, duplication, use, or modification.

Openness. There must be openness and clarity surrounding data management and practices.

Individual Access. Individuals should be able to access information about them, as well as challenge its accuracy and completeness. Information should be amended as necessary.

Challenging Compliance. Individuals can challenge the organization's compliance based on the above-mentioned principles.

APEC Privacy Framework

The APEC Privacy Framework was developed to provide free information flow for continued trade and economic growth in the Asia Pacific Economic Cooperation region while ensuring privacy protections [19]. It is comprised of 9 principles which are detailed below [20].

Preventing Harm. Protections must be put in place to prevent the wrongful use or collection of personal information. Safeguards must be proportionate to the amount of harm that could be done.

Notice. Individuals must be notified before or when their information is being collected. In the case they cannot be notified at that time, notice must be given within a reasonable timeframe.

Collection Limitation. Personal information must be collected lawfully and fairly, and only for the purpose in which it is being used. In some cases, with notice or consent of the individual is required.

The Use of Personal Information. The use of personal information is limited to the purposes in which it was collected or other related purposes.

Choice. Individuals should have a choice when it comes to the collection, use, and disclosure of their data. If information is publicly available there is an exception.

Integrity of Personal Information. Information should be accurate, complete, and kept up to date.