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/eai.26-5-2020.166352

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

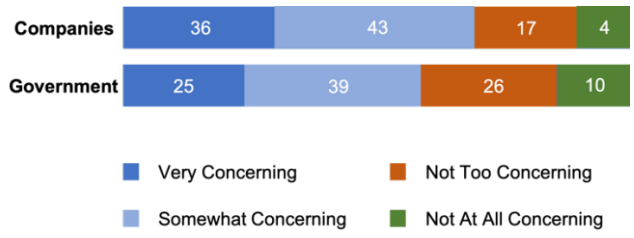

Figure 1. Data Usage Concerns

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.

Security Safeguards. Security safeguards that are proportional to the risk of potential harm must exist for personal data. They should be assessed periodically.

Access and Correction. Individuals can access their personal information and challenge its accuracy [20]. In the case information is inaccurate, individuals can request a correction. If accessing data is a burden or making a correction presents risks, there is an exception [20].

Accountability. The data controller must comply with the regulation and can be held accountable in the case of noncompliance.

Federal Data Protection Law

Mexico's Federal Data Protection Law went into effect in 2011 to protect personal data that is being held by private parties [21]. Below are the key items set forth in the law.

1. Data controllers must adhere to the regulation principles laid out, specifically when it comes to legality, consent, notice, quality, purpose, fidelity, proportionality, and accountability.

2. Personal information must be collected and processed lawfully and truthfully.

3. Individuals must consent to the use of their data and have the ability to revoke consent at any time. For sensitive personal data, written consent is needed.

4. Data must be kept accurate and up to date.

5. Data should only be kept as long as it fulfills its purpose [21]. Information about "nonperformance of contractual obligations" must be removed after 72 days of nonperformance.

6. Data can only be processed in the way it is described in the privacy notice. In the case the organization decides to process it differently, the individual must be notified.

7. Individuals must be notified as to what information is collected about them and why. This must be stated in the privacy notice.

8. Privacy notices must include information on the identity and domicile of the data controller; the reason for data processing; limitations of data use or disclosure; individual rights of access, cancellation, or objection; data transfers; and how individuals will be notified about privacy notice changes.

9. Individuals should be notified about changes in the privacy notice that are related to how data is obtained.

10. Organizations must take the proper measures to safeguard information and prevent "damage; loss; alteration; destruction; or unauthorized use, access, or processing" of data. Risk and consequences should be taken into consideration when implementing safeguards [21].

11. Security breaches must be reported immediately to the data owner.

12. Confidentiality of the data must be maintained by the data controller.

Data Privacy Act

The Philippines Data Privacy Act was passed in 2012 to protect individual privacy while still "ensuring the free flow of information for innovation and growth" [22]. The regulation was updated in 2016 [22]. The law applies to organizations with offices in the Philippines or organizations that process data in the Philippines. It applies to all citizens of the Philippines regardless of their current place of residence. It does not include the processing of information in the Philippines that was legally collected from foreign residents [22]. Below are the key items set forth in the law.

1. A National Privacy Commission must be implemented.

2. All data should be processed in a transparent, purposeful, and proportional manner.

3. Data must be collected for legitimate purposes that are known to the individual. Consent is need for the collection of personal data. The individual must understand the purpose for which their data is being processed and be aware of any use for profiling, marketing, or sharing. Additional consent is needed for data sharing. Consent is not needed if information is fulfilling a contractual agreement, protecting the data subject, or being used to "respond to a national emergency".

4. Shared data must be accompanied by an agreement that safeguards the data subjects.

5. The Philippines Human Security Act of 2007 must comply with the Act.

6. Privacy and security programs must be created.

7. Individuals can request the deletion of their data from a database. Individuals have additional rights and the ability to take action if data is "inaccurate, incomplete, outdated, false, unlawfully obtained", or used in an unauthorized fashion. They also have rights related to data portability.

8. A data breach must be reported to data subjects and the National Privacy Commission within 72 hours if sensitive information that can be used for identity fraud was obtained, there is a belief that an unauthorized acquisition has occurred, there is a belief that significant harm can occur, or the risk to the individual is real. Failure to notify the parties can result in significant penalties [22].

Personal Data Protection Act 2012

Singapore's Personal Data Protection Act was passed in 2012 [23]. Its objective is to regulate the collection and usage of personal data [23]. Below are some key items set forth in the law.

1. Personal data can only be collected for purposes an individual would find reasonable and appropriate.

2. Individuals must be notified of the purposes for which data is collected. Notification must take place before data is collected, used, or disclosed. Consent can either be expressed or implied. Consent can also be withdrawn, but any legal consequences will be the responsibility of the individual [24].

3. Individuals have the ability to control and access their personal data. They are able to correct, block, and request erasure. Organizations can choose not to correct the data, but there must be a note that the data was not changed. When it comes to erasure, requests may be considered when data no longer serves a purpose. In the case the data is publicly available, it is possible that data will not be erased [24].

4. There must be reasonable security to protect data and prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or other risks.

5. Transfer of data outside of Singapore is limited.

Protection of Personal Information Act

South Africa's Protection of Personal Information Act was signed into law in 2013 and covers the jurisdiction of South Africa [25]. It addresses both personal information and information related to juristic persons [25]. Below are the key items set forth in the law.

1. Personal information must be processed lawfully and reasonably.

2. Data must be collected for a specific, defined purpose and the individual must be notified.

3. Additional processing of the information must be related to the original processing.

4. Organizations must take the necessary steps to ensure the quality of personal information is maintained. All information should be complete, accurate, up-to-date, and not misleading [26].

5. Individuals must consent to the collection of personal data and must be notified about collection.

6. Documentation of processing operations is mandatory.

7. Individuals must have access to their personal information.

8. Security safeguards must be in place to protect the integrity and confidentiality of data [26]. In the case of a breach, parties must be notified "as soon as reasonably possible".

9. A Data Protection Officer is required at all organizations. The individual must register with the Information Regulator [25].

Turkish Data Protection Law

The Turkish Data Protection Law was born from the European Union Directive 95/46/EC, also known as the EU Data Protection Directive (1995) [27]. Below are some key items set forth in the law.

1. There must be a specific purpose for the processing of personal information. Any further processing is prohibited. If other reasons present themselves, the data controller will need to receive consent from data subjects.

2. Consent is needed for the processing of both sensitive and non-sensitive data.

3. Sensitive and non-sensitive personal data can be transferred outside of Turkey; however, the receiving country must have adequate data protection and both parties in the transfer must commit to protecting the information.

4. Data controllers must register with the Data Controller's Registry. Policies must be presented [27].

Cybersecurity Law

The Cybersecurity Law of China was passed in 2016 [28]. The law addresses how organizations should approach privacy and security for personal data. Below are the key items set forth in the law [28, 29].

1. The proper security safeguards must be put in place. A layout and requirements for cybersecurity are provided and key infrastructure is included.

2. Individual privacy must be achieved. The collection and usage of personal data is standardized in the law.

3. Domestic storage is required for all sensitive data.

4. In the case organizations violate the law, they will incur penalties.

5. Individuals have the right to request corrections to their data. This includes all personal data collected and stored by the organization. The necessary steps should be taken to remove or correct the individual's information.

6. All information collected requires consent and notification to the individual.

7. All collected information needs to be used legally and properly.

Personal Data Protection Bill 2019

India's Personal Data Protection Bill was passed in 2019 [30]. It includes a number of provisions to protect personal data, which are outlined below [30].

1. Data can only be processed if there is a clear and lawful purpose. This data must be processed fairly, reasonably, and only for the purpose that the individual has given consent.

2. Only data necessary for processing can be collected.

3. Organizations must ensure the data being processed is complete, accurate, up-to-date, and not misleading. Individuals are able to request corrections.

4. Personal information should only be kept for the period in which it is being processed. Following this period, it should be deleted.

5. Data fiduciaries must comply with this regulation.

6. Notice is needed at the time of data collection.

7. Individuals must be notified of breaches as soon as possible.

8. Data can be transferred outside of India only with the data subject's explicit consent [30].

3.2. Recent Data Protection and Privacy Regulations

The regulations listed below are the most recent data protection and privacy regulations. These regulations capture the majority of the mandates discussed in previous regulations and build on them further.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation was passed in 2018. It replaces the UK's Data Protection Act (1998) and the EU's Data Protection Directive (1995). There are 7 key principles of GDPR which are listed and detailed below [31, 32].

Lawfulness, Fairness, and Transparency. All data must be processed lawfully, fairly, and transparently.

Purpose Limitation. Data must be collected for specific and legitimate purposes that are explicitly stated. Data cannot be processed in ways other than what is outlined.

Data Minimization. Data collection is limited to data that is relevant for processing purposes.

Accuracy. Information must be accurate and kept up to date. Inaccurate information must be corrected or deleted.

Storage Limitation. Data should be kept no longer than what is necessary for processing.

Integrity and Confidentiality (Security). Appropriate organizational and technical safeguards must be put in place to protect data from unauthorized or unlawful processing, loss, destruction, or damage [32].

Accountability. Data controllers are responsible for GDPR compliance and are held accountable for ensuring the proper measures are in place [32].

Personal Data Protection Act

The Thailand Data Protection Act was passed in 2019 and goes into effect in 2020 [33]. The regulation applies to organizations that offer products and services in Thailand or track individuals in Thailand [33]. The key items set forth in the law are detailed below.

1. Organizations must have a legal reason for the collection and usage of personal data. In some cases, consent is required.

2. Appropriate security safeguards must be implemented to protect personal data. In the case of data breaches, notifications must be provided.

3. Individuals are able to exercise their rights regarding their personal information.

4. For sensitive personal data, additional safeguards are needed to protect privacy.

5. In some cases, a Data Protection Officer must be appointed.

The California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act was passed in 2018 and went into effect in 2020 [34]. The regulation applies to organizations that do business in California and process the data of California residents [35]. The key items set forth in the law are detailed below.

1. Individuals have the right to know when their data is being collected and used.

2. Individuals have the right to know if their information is sold or disclosed. They also have the right to know the names and addresses of the parties their data is being shared with.

3. Individuals have the right to access their personal data. They also have the ability to request copies of their data.

4. Individuals cannot be discriminated against for practicing their privacy rights.

5. Individuals have the right to know what type of personal information is being collected, as well as what specific information.

6. Individuals have the right to request deletion of their personal data.

7. Individuals have the right to know the source of collection of their personal data.

8. Individuals have the right to know why their personal data is being collected or sold.

9. Individuals have the ability to opt-out of the collection, sharing, or sale of personal data.

10. Organizations need explicit consent for collecting and selling information about minors [36].

11. Individuals have the right to sue organizations that do not comply with CCPA [36].

Brazilian General Data Protection Law

The Brazilian General Data Protection Law was passed in 2018 and goes into effect in 2020 [38]. It applies to both public and private organizations that "process personal data in Brazil", "process personal data that was collected in Brazil", or "process personal data to offer or provide goods or services in Brazil" [38]. The key items set forth in the law are detailed below.

1. Personal data can be processed if individual consent is received, it is needed for contract fulfillment, there is a legal obligation, it is needed for research studies, it is needed for health care purposes, or it effects the physical safety of an individual. Sensitive information can only be processed with consent.

2. Individuals have the right to request access to their personal data; deletion of personal data that was processed without consent; corrections to incomplete, inaccurate, or stale data; and anonymization, blocking, or deletion of data processed in ways not complaint with the regulation. It also applies to data that was collected in excess [38].

3. Individuals have the right to transfer personal data between service or product providers.

4. Individuals have access to information about the parties their personal information is shared with.

5. Any data transferred outside of Brazil must have adequate protection.

6. Data transferred outside of Brazil requires consent from the individual or contractual instruments.

7. An individual must be put in charge of processing the data [38]. They will be liable for regulation compliance [38].

3.3. Upcoming Data Protection and Privacy Regulations

Many countries are putting significant effort into amending their existing data protection and privacy regulations, while others are working to develop new regulations. Some of the most notable upcoming regulations are listed below.

Act on the Protection of Personal Information

Japan's Act on the Protection of Personal Information was passed in 2003 and updated in 2015. The cabinet of Japan recently approved a bill for further amendments to the Act [39]. The key items set forth in the law and proposed amendments are listed below.

1. Data subjects can request that organizations stop using, delete, or stop the transfer of information that was used for purposes other than those originally stated [39]. This also applies to information used improperly or in violation of the original Act on the Protection of Personal Information. The new amendment will increase the scope, allowing these requests when an individual believes their interests are likely to be violated.

2. Individuals can request access to their personal data, as well as records about data sharing with third parties.

3. Any personal data will be considered retained regardless of the retention timeframe.

4. Under the original Act on the Protection of Personal Information, data subjects needed to consent to the sharing of data with third parties. The amendment will utilize opt-out to restrict the data that could be shared. Data collected deceitfully or improperly cannot be shared. In addition, data received under an opt-out scheme cannot be used.

5. In the case of a data breach, data subjects must be notified if their rights and interests will be violated.

6. Personal data cannot be used in ways that "encourage or cause the unlawful or undue use of data".

7. Pseudonymized information will be used to ensure a specific individual cannot be identified by the data. This mandate is limited to the organization.

8. When it comes to sharing data, the recipient of the data must confirm that consent was given by the individual to share their data.

9. If data is transferred outside of Japan, the receiving organization must provide information on the data protection system that country has in place.

10. Organizations must detail and notify individuals as to how their information is being used. Consent is needed from individuals when information is being used for purposes other than what was originally stated. Information must be obtained in a lawful and truthful manner.

11. The necessary measures must be taken to prevent data breaches, as well as loss or damage to information.

Data Security Administrative Measures

In May 2019, the draft of China's Data Security Administrative Measures was released [41]. Personal and important information (information that could significantly impact national security, social stability, public health, public security, and economic security) are covered in the regulation. The regulation was developed to supplement China's Cybersecurity Law and Personal Information Security Specifications [41]. It further addresses notice and consent, registration requirements, exceptions for personal information disclosures, guidelines for the collection and use of personal information, data breaches, cross-border transfers, penalties, and additional measures for data and activities.

The regulations listed above are the primary data protection and privacy regulations around the globe. While some regulations may include additional principles, the key principles have been identified. It is also important to note that there may be exceptions to some of the identified principles.

3.4. Common Principles Found in Data Protection and Privacy Regulations

Figure 2 below summarizes the primary principles that are found in data protection and privacy regulations.

Principle	Definition
Openness and Transparency	Refers to openness and transparency when it comes to the collection, usage, storage, or sharing of personal data.
Fair, Lawful, Adequate, Relevant, and Reasonable Use	Refers to the fair, lawful, adequate, relevant, and reasonable use of personal data.
Notification	Refers to notification of data practices, including collection, usage, storage, or sharing. It could also include notification of changes to practices.
Safeguards	Refers to the safeguards that must be put in place to protect personal data from unauthorized access, abuse, theft, loss, accidental access, unauthorized processing, and/or unauthorized erasure.
Consent	Refers to consent that is needed or requested for the collection, usage, storage, or sharing of data. This could include opt-in or opt-out.
Data Quality and Accuracy	Refers to the maintenance and assurance of personal data quality. This could include an individual's ability to request corrections to personal data or deletion.

Storage and Retention	Refers to the retention and storage of personal data. This could include storage timeframes, the type of data that is stored, and general storage practices.
Data Access	Refers to individuals having access to their personal data.
Cross-Border Transfer	Refers to the requirements related to transferring personal data outside of the current region.
Government Related Identifiers	Refers to the use, disclosure, or adoption of government related identifiers.
Data Collection	Refers to requirements and limitations related to the purpose, source, and manner of personal data collection.
Appointments of Officers and Commissions	Refers to the appointment of officers and commissions to manage personal data and maintain responsibility for regulation compliance.
Reporting of Breaches	Refers to time frames in which data breaches must be reported.
Right to Be Forgotten	Refers to the right for an individual to have their personal information removed from applications, storages, searches, etc.
Purpose Limitations	Refers to limitations on how personal data can be processed.

Figure 2. Main Principles Found in Data Protection and Privacy Regulations

Identifying the most common principles found in regulations helps in understanding the purpose and goals of data protection and privacy regulations. As global governments gain more knowledge about how data collection, processing, and retention threaten privacy and have other negative impacts, more regulations will be amended, drafted, and passed. This will result in an expansion of the common principles.

4. Challenges Presented by Regulations

The safeguards found in data protection and privacy regulations have made compliance challenging. Many of these specific challenges have been identified and detailed below.

4.1. Understanding and Acting on the Broad and Vague Context of Regulations

Many regulations are written in a broad and vague context. This requires them to be deciphered. A recent GDPR related survey identified "deciphering expectations" as the largest challenge for organizations [6]. It was noted that many feel GDPR is extremely broad and could apply to all data on individuals [42]. According to another study, some provisions in CCPA are considered "too broad" and/or "vague" [43].

Organizations must have a thorough understanding of regulations in order to decipher them. Once this is achieved, organizations need to determine whether the regulations apply to them, what areas in which the regulations apply, and what they need to do to comply in both a broad and granular sense.

This could be extremely taxing for organizations, especially small and mid-size enterprises (SMEs) with small departments, large work loads, and limited resources.

4.2. Translating Regulations into a Technical Context

Regulations are written in a non-technical context. According to a GDPR study, this qualitative approach results in a lack of clarity [6]. Organizations must try to decipher and understand the objectives of the regulations. They then need to identify the technical steps that need to be taken to achieve those objectives.

Like the previous challenge, this could be extremely taxing for organizations, especially small and mid-size enterprises (SMEs) with small departments, large work loads, and limited resources.

4.3. Overcoming Technical Challenges

There are several technical challenges when it comes to complying with data protection and privacy regulations.

Identification of Security Controls

Many of the regulations mandate security controls, which could include encryption, data anonymization or pseudonymization, and access and identity management, among others [44]. The regulations do not identify specific controls, which leaves this requirement open to interpretation. In addition, these safeguards could take time to put in place and can be especially challenging for organzations that have limited resources or are not security focused.

Managing Data

Organizations need to have a clear understanding of their data flow mapping [6]. This gives them insight into how data behaves and where it is stored [6]. In turn, organizations can control data and protect it [6].

An example of this challenge can be found when trying to comply with GDPR's "right to be forgotten". Individual information can be exchanged and kept on multiple applications including emails, databases, files, etc. [45]. It can also be found in onsite or off-site storages [45]. When data controllers or individuals responsible for managing data receive a "data removal request" they need to know where to go to delete it.

It is important to note that organizations that take the necessary steps to understand data behavior may unearth larger challenges that need to be addressed (e.g. the use of extremely risky data practices) [6].

Lack of Automation

In many cases, organizations are using manual processes and workflows. This is especially true when it comes to data mapping and tagging [6]. Automation is needed to have an efficient and effective process, and ease the challenges that come with data protection and privacy regulation compliance.

It is believed that automation could facilitate technical compliance in the case of GDPR [6]. When data controllers or individuals responsible for managing data receive a "data removal request" they must manually search for, identify, and remove the data [45]. This needs to be done in both the production and back up environment [45]. Automated processes and workflows could simplify the process; however, organizations will need to have significant resources to implement them.

Updating Proprietary Technology

Many organization have internally built proprietary technology. Unlike vendor provided platforms, organizations will need to take on the task of updating systems so they are compliant. This will take both time and resources.

Deleting Information on Backups.

Backing-up data is a process that happens repeatedly to ensure organizations have copies of up to date information. This process is critical for business continuity, as it enables the quick recovery of systems and data when they are damaged or lost due to malicious actions, hardware failures, systems crashes, etc [45].

As previously mentioned, GDPR includes the "right to be forgotten". This requires information to be deleted from back-ups, which is extremely challenging and sometimes impossible.

Data can not be erased from optical disks [45]. New back-ups need to be made every time an individual requests the removal of their data [45]. All previous disks must also be destructed [47]. In the case of hard disks, the relevant data needs to be deleted on the current storage and all backups need to be altered [48]. When it comes to tape disks that cannot be randomly accessed, the whole database needs to be restored [49]. This is both costly and complex [45]. It can also take a significant amount of time.

4.4. Complying with Multiple Regulations with Different Requirements

There are many data protection and privacy regulations throughout the world, each having different requirements for compliance. This makes it challenging for organizations to implement and manage the proper controls.

The scope of information covered by regulations is a primary example. Recent regulations are expanding personal data to include IP address, location, biometrics, and genetic information [46]. Another example, is some regulations mandate one action and process, while another mandates the opposite action and process. GDPR requires individuals to "opt-in" for data collection, while CCPA automatically infers individuals are opted-in and requires that users have the ability to "opt-out". This requires organizations to have two different workflows in place, which can be difficult to manage.

4.5. Updating, Monitoring, and Managing Workflows and Processes

Workflows must be developed or updated to achieve data protection and privacy regulation compliance. In addition, the organization needs to continuiously manage these workflows.

This could be a learning curve for organizations. It also requires a significant amount of resources. This can be especially taxing for SMEs who may not have dedicated teams in place and/or have minimal budgets.

There are many challenges related to data protection and privacy regulation compliance, including understanding and acting on broad and vague regulations; translating regulations into a technical context; updating, monitoring, and managing workflows and processes; and complying with multiple regulations at once. There are also technical challenges that organizations face. Understanding these challenges is important, as it will assist achieving data protection and privacy in the long-term.

5. Recommendations

The previous section identifies some of the challenges organizations face when trying to comply with regulations. This section presents recommendations to mitigate the challenges and achieve data protection and privacy in the long-term.

5.1. Provide Detailed and Precise Requests in Regulations

Many data protection regulations are broad and vague in context. This leaves room for interpretation. In order to avoid misinterpretation and achieve desired compliance, regulations need to be clear and concise about objectives and what needs to be done to achieve them.

For example, many of the regulations require that personal information only be kept as long as it is being used. More clarity is needed on this statement, specifically around the word "used". Organizations need to understand what does and does not constitute data usage to prevent the storage of information for nonsensical reasons. There should also be a maximum time frame provided for the retention of personal data. After this period, personal data must be destroyed, or additional consent must be given. This will prevent information from being stored for

extensive periods of time, which will result in inaccurate or out of date information. In the case of a data breach, this would reduce the amount of information that is taken.

5.2. Identify Technical Requirements and Provide Support

Current regulations do not include any technical information. They are strictly presented in non-technical language. This makes regulations challenging for IT teams to decipher and leaves room for interpretation when it comes to the appropriate approach that needs to be taken. The specific controls that need to be implemented should be identified, as well as the type of data the controls need to be applied to.

In addition, IT teams should be provided with best practices and acceptable standards for these controls. These can come in the form of regulation companion guides.

Many organizations would benefit from the ability to speak with an expert on regulations. For this reason, there should be designated agencies or teams within agencies that can respond to questions or provide hands on support. This is the case for some existing regulations, but not all.

These additions will clarify what controls regulators deem appropriate; ensure the controls and safeguards provide appropriate protection for the data; and provide overall support for organizations, which would help ensure the regulations are being adhered to.

5.3. Establish a Global Agency to Address Data Protection and Privacy Regulations and Standards

A global agency should be developed to oversee data protection and privacy. This agency would be responsible for advocating for data protection; monitoring the risks related to the collection, usage, and sharing of personal data; establishing structure and principles for data regulations; and helping to ensure the overall protection of an individual's personal data. Having one centralized agency will help identify specific objectives and streamline regulations. This could mitigate the piecemeal approach that is currently taking place and providing a number of challenges.

5.4. Identify Long-Term and Short-Term Objectives and Set Reasonable Time Frames for Compliance

Some of the most recent regulations require drastic and expensive changes to be made in short timeframes. For example, the "right to be forgotten" would require personal data to be deleted from backups. Depending on how data is backed up, this could be extremely challenging or impossible for organizations to achieve in the short-term, as they may have to update their entire backup process.

In order to protect data in the long-term, both short-term and long-term objectives must be set. Items like the "right to be forgotten" could be broken down into long-term and short-term objectives. For example, all back-up processes must be of a certain standard within two years of the regulation passing and all organizations must adhere to the "right to be forgotten" within four years of the regulation passing. Other short-term objectives could address personal data collection and usage.

The abovementioned recommendations will assist regulators in developing regulations that organizations can comply with more seamlessly. In addition, they can provide a more long-term vision for data protection and privacy.

6. Conclusion

Individual privacy and protection has been a concern for many years. As the collection and usage of personal data increases, regulations are passed and amendments are made. Many of these regulations have presented a number of challenges for organizations.

In this paper, we identified different data protection and privacy regulations, as well as the compliance challenges organizations face. This was necessary in order to provide recommendations that can be used to develop future regulations, make amendments to current regulations, and achieve overall data protection and privacy in the long-term.

Future work should consider studying the recommendations on a more granular level, including specific security controls that should be implemented; contents of companion guides; and the identification of responsibilities, objectives, and a framework for a global data protection agency. Future studies can also be done on data protection and privacy regulation challenges in IoT.

References

[1] Solove, D. J. (2016). A brief history of information privacy law. Proskauer on privacy, PLI.

[2] Choi, J. P., Jeon, D. S., & Kim, B. C. (2019). Privacy and personal data collection with information externalities. Journal of Public Economics, 173, 113-124.

[3] https://www.businessinsider.com/invasion-of-data-privacy-online-in-person-examples-2020-1#make-no-mistake-this-data-is-valuable-in-2018-american-companies-spent-an-estimated-19-billion-getting-and-analyzing-consumer-data-third-parties-known-as-data-brokers-collect-the-information-and-sell-it-2

[4] Brown, B., Kanagasabai, K., Pant, P., & Pinto, G. (2017). Capturing value from your customer data. McKinsey & Company.

[5] https://www.pewresearch.org/internet/2019/11/15 /americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/

[6] Sirur, S., Nurse, J. R., & Webb, H. (2018, January). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR).

In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (pp. 88-95).
[7] Presthus, W., Sørum, H. & Andersen, L.R.: GDPR Compliance in Norwegian Companies (2018). Paper presented at NOKOBIT 2018, Svalbard, 18-20 Sept. NOKOBIT, vol. 26, no. 1, Bibsys Open Journal Systems, ISSN 1894-7719.
[8] https://iapp.org/news/a/gdpr-matchup-australias-privacy-act-1988/
[9] https://www.marketing.org.nz/Resources/Article?Action=View&Article_id=16
[10] https://iapp.org/news/a/gdpr-matchup-new-zealands-privacy-act-1993/#
[11] https://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC
[12] https://iapp.org/news/a/gdpr-matchup-hong-kongs-personal-data-privacy-ordinance/
[13] https://www.cdc.gov/phlp/publications/topic/hipaa.html
[14] https://www.total-shred.com/the-data-protection-act/
[15] https://privacyrights.org/resources/gramm-leach-bliley-act-basics
[16] GRAMM-LEACH-BLILEY ACT. https://www.sec.gov/about/laws/glba.pdf
[17] https://digitalguardian.com/blog/what-pipeda-personal-information-protection-and-electronic-documents-act-understand-and-comply
[18] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles
[19] https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/
[20] Raul AC. The privacy, data protection and cybersecurity law review. English. 2014. ISBN: 978-1-909830-28-8
[21] Executive Branch, Ministry of the Interior. DECREE issuing the Federal Law on Protection of Personal Data Held by Private Parties and amending Article 3, Chapter II of Title II of the Federal Law on Transparency and Access to Public Government Information. https://iapp.org/media/pdf/knowledge_center/Mexico_Federal_Data_Protection_Act_July2010.pdf
[22] https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/
[23] CHIK, Warren B.. The Singapore Personal Data Protection Act and an assessment of future trends in data privacy. (2013). Computer Law and Security Review. 29, (5), 554-575. Research Collection School of Law.
[24] https://iapp.org/news/a/gdpr-matchup-singapores-personal-data-protection-act/
[25] https://iapp.org/news/a/gdpr-matchup-south-africas-protection-of-personal-information-act/
[26] Van Aswegen, L., Kirkland, A.. How to Comply with South Africa's Protection of Personal Information Act (2015) Trustwave Holdings
[27] https://iapp.org/news/a/gdpr-matchup-turkeys-data-protection-law/
[28] https://iapp.org/news/a/gdpr-matchup-chinas-cybersecurity-law/
[29] IT Advisory KPMG China, Overview of China's Cybersecurity Law, February 2017
[30] https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf
[31] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
[32] https://www.privacypolicies.com/blog/gdpr-privacy-principles/
[33] https://www.insideprivacy.com/data-privacy/thailand-passes-personal-data-protection-act/
[34] https://iapp.org/resources/topics/california-consumer-privacy-act/
[35] https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/
[36] https://360advanced.com/what-is-ccpa/
[37] https://iapp.org/resources/article/california-consumer-privacy-act-of-2018/
[38] https://www.natlawreview.com/article/6-months-until-brazil-s-lgpd-takes-effect-are-you-ready
[39] https://iapp.org/news/a/analysis-of-japans-approved-bill-to-amend-the-appi/
[40] https://www.loc.gov/law/help/online-privacy-law/2012/japan.php
[41] https://www.endpointprotector.com/blog/chinas-data-security-administrative-measures/
[42] https://www.dfinsolutions.com/insights/article/deciphering-gdpr-dfin-primer
[43] https://www.nbcnews.com/tech/tech-news/california-bringing-law-order-big-data-it-could-change-internet-n1005061
[44] https://www.mckinsey.com/business-functions/risk/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge
[45] Eugenia Politou et al., Backups and the right to be forgotten in the GDPR: An uneasy relationship, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.08.006
[46] https://cloud.netapp.com/blog/how-data-protection-regulations-impact-enterprise-storage-management-blg
[47] Ge, Yong-Feng, Jinli Cao, Hua Wang, Jiao Yin, Wei-Jie Yu, Zhi-Hui Zhan, and Jun Zhang. "A benefit-driven genetic algorithm for balancing privacy and utility in database fragmentation." In Proceedings of the Genetic and Evolutionary Computation Conference, pp. 771-776. 2019.
[48] Chenthara, Shekha, Khandakar Ahmed, Hua Wang, and Frank Whittaker. "Security and privacy-preserving challenges of e-health solutions in cloud computing." IEEE access 7 (2019): 74361-74382.
[49] Shu, Jiangang, Xiaohua Jia, Kan Yang, and Hua Wang. "Privacy-preserving task recommendation services for crowdsourcing." IEEE Transactions on Services Computing (2018).