IE2022 – Introduction to Cyber Security.

Sri Lanka Institute of Information Technology.

Year 2 Semester 1

Individual Assignment - 2023

Submission Data: 15/05/2023

Nanayakkara Y.D.T.D

IT21826368

Data Privacy Rules

Abstract.

Data privacy is the protection of personal information and the right of individuals to control the collection, use, and sharing of their data. Data privacy rules are the set of regulations and laws that govern the collection, use, storage, and sharing of personal information. Understanding data privacy rules is crucial in today's digital age. With the increasing amount of personal data collected and processed by organizations, it is essential to ensure that data is used ethically and in compliance with legal and regulatory requirements.

In many countries, data privacy rules are enforced through legislation such as the GDPR in the European Union, the CCPA in California, and the Personal Data Protection Act in Singapore. These regulations set out specific requirements for organizations that collect and process personal data, including obtaining consent, providing transparency, and implementing appropriate security measures.

Finally, you will understand, getting more understanding on data privacy rules are way to improve data security and protection, greater transparency in data processing practices, increased accountability and responsibility in data handling, and enhanced trust between businesses and consumers. Overall, a strong understanding of data privacy rules is essential for protecting personal information and maintaining a healthy and trustworthy digital economy.

Table of Contents

1. Introduction.

> "They are watching us. They know I am writing these words. They know you read them. Governments and hundreds of co-operations are spying on you and me, and everyone we know" [1].

In every minute around the world the data is being processed, shared, collected, and destroyed as an act of information communication. These data have ownership and a purpose. The ownership of the personal data, including controlling, managing, and processing is a human right which every human will get. As you can see once's privacy is more integrated in this. The privacy is more than an interest or preference. Privacy's moral weight, its importance as a value for a person who wants and likes it, or how much they want or likes it does not shrink or swell in direct proportion to the numbers. Taking privacy as a serious matter because it is among the human rights, duties, or values of any morally legitimate social and political system. So, protecting this right is a necessity and will need more controlling and security.

Agreeing that data privacy is a main important part which can lead to construct these rules and regulations. These rules help to establish trust between individuals and the organizations that collect and process their data. They provide guidelines for the collection, processing, and use of personal data and outline the consequences for non-compliances. Internationally, or for each country digital data privacy rules were implemented by the governments and organizations. There are various laws and regulations in place, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Personal Information Protection and Electronic Documents Act (PIPEDA).

Let us see then how the data privacy rules are crucial to protect individuals' privacy rights and prevent the misuse of personal data in this evolving world and dive deeper into each of these areas, providing a further explanation and an overview of the current statues of the data privacy and its rules.

2. What is Data privacy?

Data privacy can be explained simply by the ability which a person to determine for themselves when, how, and to what extent personal information on them is collected, shared with, or communicated with world and be able to in control. This Personal Information can be one's name, location, contact information, medical records, personal sensitive information or online or real-life behavior.

In one point data privacy is a messy and a complex subject to look at. The protection of information on the internet is a one way to called it. It is also the practice of using the internet privately without leaking or compromising own or others information. It applied to various context, information sharing to messages and private communications. So, it is necessary to explore the data privacy, its importance and how the individuals and organizations keeping them safe.

2.1.Importance of the Data privacy.

The internet is primary funded by the collection, analysis and trade of data – the data economy [1] Many users using internet wants to control and prevent certain types of these personal information collection because of the importance of the data which can be used for various purposes. The purpose can be good or can be bad either way it can affect the person. It can compromise one's security and privacy. No one wanted to share details about themselves with strangers. Data which are gathered and shared without consent can be a violation of human right according to that fact.

Due to the expand international flows of the personal information, the stakes are being increasing for United States and European Union to produce the data privacy laws. As according to one estimate, the US-EU economic relationship involves $260 billion annual digital services in trade [2].

2.2.Why collect data and Importance.

"Data is the key to unlocking value in the digital age." - Satya Nadella, CEO of Microsoft.

We can say the data is the fuel of every technology we use in day-to-day life. Data collection is a key role in the cyberspace; hence the whole industry depends on the data. It becomes the nature of the data. The processed data is known as the information we used for everything in the digital space. Collection data is important because of the common key factors like Improving the user experience, Analytics and research for future developments, Security and fraud prevention, innovation, Efficiency and productivity, communication, and entertainment. So, the basic infrastructure will be the data which collected.

2.2.1. Data Ownership.

Data will be collected by governments, Organizations, Businesses and individuals to do various tasks. These collected data will need to be safeguard. It will be needed in control and managing.

When an organization or an enterprise collects own personal information, they have more control over the once's personal information in sharing and who has the access to it. This helps in privacy protections but not automatically guarantee completely. Still, they have the responsibility to protect that data and to comply with applicable data privacy and regulations. So, the data ownership will be the next question comes upfront.

Both possession and responsibility for information ownership is a no easy answer question. Indeed, debates about the subject tent to be theoretical. Depending on the Situation, the processor, the user, the creator, and the subject of the information could all clam the ownership. Because of the Organizations and enterprises become more reliant on the data, the monitoring or auditing the data ownership should ascertain whether the data ownership is the attention of top management or whether there are guidelines addressing the use of data and the decision making associated with data ownership [3].

"due to the sheer volume of data and the complexity of their movements, it may not be feasible for an enterprise to identify the owner of every piece of datum it possesses at any given time." [3]. The sharing of data and use of personal information now drives on many daily activities including finances, health care, shopping, telecommunications, and transportation. Every leading IT and technology companies are depending in these data accesses, and use of information.

2.2.2. Management risks related to Data Ownership.

In addition to knowing the nature of the data created, collected, processed, and stored there are ways that enterprises can mitigate the risk associated with data ownership. These strategies are combined with the fundamental of good data governance [3].

- Accountability.

Responsibility and accountability are defined roles from the chief information officer and data protection officer does. These individuals are responsible for the management of the small subsets of the data which are critical to managing the risks in data ownership.

- Information Security.

Whether the data is owned by the organization or by an outside entity, loss, theft, and unauthorized access are immediate risk considerations connected with its ownership. To make sure that data is protected while in the hands of the organization, internal auditors and risk managers should collaborate closely with information security teams.

“GDPR raised the stakes in terms of the extent to which an enterprise or data controller is responsible for the use and misuse of data by external parties.” [3].

- Data Retention policy.

The importance of the data retention strategy stems from the fact that, as was already mentioned, the ownership and possession of data entails risk. A retention policy guarantees that the company only has data that is useful to it. The policy ought to be reviewed for compliance on a regular basis [3].

- Consent and Disclosure.

Consent and disclosure are essential, especially in the post-GDPR environment, when it comes to the risk of owning data that belongs to other people. To reduce the potential of future legal or reputational liability, the organization should obtain consent to gather data and disclose how those data will be used [4].

- Third-Party Contracts.

Regarding the degree to which an organization or data controller is liable for the use and misuse of data by third parties, such as vendors who handle data on the controller's behalf, GDPR raised the stakes. To make sure that contracts with external data processors comply with GDPR and that the company has visibility into the processor's capacity to retain records of personal data and how those data are handled, internal auditors should analyze contracts with those processors. Furthermore, if data are shared with a third party, that company might utilize the data in other ways. In that instance, agreements that lay out the parameters for ownership, usage, and sharing should be in place [3].

Mostly knowing the data ownership helps with the compliance with regulations. Many organizations will need to require a clear data ownership policy in the first place. For Example, GDPR in Europe Union requires Organizations to designate a Data Protection officer (DPO) to oversee with the regulation itself [4]. When managing disputes over the data ownership having clear ownership policies are in place can be another reason to know the data ownership. In data sharing and clarify the responsibilities also it takes a major advantage. These data collecting organizations, businesses can have different processes and visions due some factors like difference interests in people, cultural or regional differences.

2.3.Different Vision of Data privacy.

When the frameworks were developed around different environments do the vision will be going along. As an example, think of a two systems of data privacy rules envision the individual from the perspective of an anthropologist, law is a species of social imagination As Clifford Geertz observes. Legal thoughts constructive of social realities and merely reflective on them. The shared cultural background forms a key part of juridical decision making and even finds the settings for its problem. [2]

Whether it is a choice or not, like or did not care about the data privacy concerns were more likely to differ around the globe, even there are similar in one's perspective. Mostly these regulations were safeguarding the people data privacy.

3. Data privacy rules.

3.1.History.

Data privacy rules dates back to the early 1970s when concerns began to emerge over the increasing use of computers and the potential impact on personal privacy. One of the earliest attempts to address these concerns was the US Privacy Act of 1974, which established safeguards for the collection, use, and disclosure of personal information held by federal agencies. then several other countries also enacted laws to protect personal privacy, including the Canadian Privacy Act in 1983 and the Australian Privacy Act in 1988. However, these laws only applied to government agencies, and it was not until the rise of the internet that data privacy became a pressing issue for businesses and individuals alike.

The advent of the internet and the increasing use of digital technologies for collecting, processing, and sharing personal data prompted the need for more comprehensive data privacy laws. In 1995, the European Union enacted the Data Protection Directive, which established a framework for protecting personal data across all member states. The directive required that personal data be collected and processed only for specific purposes, and individuals had the right to access and correct their personal information.

In 2018, the EU introduced the General Data Protection Regulation (GDPR), which is considered one of the most comprehensive data privacy laws to date. The GDPR strengthened the rights of individuals to control their personal data and imposed hefty fines for non-compliance. The need for data privacy rules has arisen due to the vast amounts of personal information being collected and processed by companies, governments, and other organizations [4].

3.2.Purpose and Importance.

Principles which set out a basic framework for the processing of 'personal data' which is more defined as information related to an identified or identifiable natural person or also can called a 'data subject' can be called as the purpose of these rules. These aimed to ensure the protection of personal data, ensure to respect the human rights, protect vulnerable populations, prevent crime in any manner, assure consistent digital functionality. and fundamental freedom of individual in particular to the right of privacy.

3.2.1. Protect the vulnerable.

The global population which contains less people who are less tech-savvy and even you do not know about your digital information is misused or weaponized, how will ensure the security of the data breaches in first place?

These laws are the reason which protecting personal and businesses likely to expose their own information because the lack of understanding data privacy compliance concerns.

Each data law attempts to do this in three main ways. They are,

- Attempting to prevent the data breaches and access by prohibiting certain types of data collection.
- They restrict Companies the ability to share information that they legally collect from the consumers for transactional and information purposes.
- They penalize the wrongdoers in effort to provide justice to victims of data misuse and discourage other parties from participating in data theft.

3.2.2. Prevent Crime and Penalize.

When these laws governing data privacy prevent data breaches and hold the companies or organizations responsible for data misuse by legislating how these companies collect and process data, where they can share and store these data and how they keep promises advertised in their privacy policies which consumers have to agree before conducting online communications.

3.2.2.1. Data protection.

Combination of data privacy (how to control the data collection, use and dissemination of personal data) and data security (how to protect personal information and unauthorized access or use, responding to those) can referred as Data Protection [5]. Historically, many data privacy rules addressed these issues separately, for one for one but recent data protection initiatives indicate a combination of data privacy and security.

3.3. Challenges Faced to protect data privacy.

3.3.1. Personal Perspective.

Personally, when comes to the impact of the data breaches users face lots of challenges, even they have little control over how their personal information is used or shared, such as lack of transparency, online tracking losing control, unauthorized access**.** Which will lead to identity theft, fraud, and other privacy violations.

3.3.2. Business Perspective.

For the Businesses when it comes to the effects of the data breaches, they can make more complicated problems including cost and complexity of implementing data privacy regulations. Companies must comply with a range of legal and regulatory requirements, including obtaining consent, implementing appropriate security measures, and ensuring transparency in their data processing practices. This can cost a significant resource both in time and money.

3.4. Regulations, Policies, and practices.

When the importance of data privacy was concerned, within the evolution of the technology Data privacy rules, policies and practices were became important. Around the worldwide the governments, organizations regulatory bodies some of the common using regulations.

3.4.1. What are Laws, Rules, and regulation?

Laws, rules, and regulations are all legal guidelines that designed to govern human behavior on data collecting and processing. While they are more similar, Laws are formal legal rules enacted by a government authority like a federal or state government. As an example, in the United States, we have both Federal and State laws on data protection. Violation of a law can results a penalties like fines or imprisonment. Laws can cover a wide range of context, including criminal, civil, employment, tax, and intellectual property laws.

Rules are more less formal than laws and usually established by organizations or institutions, such as a business, government agencies. To govern the behavior within the particular context they are being used. Rules may not be a legally binding or be,

depending on the context in which they were designed and established. Violation of them may result in consequences such as suspension, termination of employment or loss or a privilege.

Regulations are specific rules or requirements established by a governmental authority, same as the rules but it has the more specific and detailed than laws. They provide guidelines how to comply with the law. Regulation violation may result in penalties such as fines or legal actions.

3.4.2. What are Frameworks.

With combinations of rules and regulations a data protection framework is a set of guidelines, a policy, which are designed to protect personal information from unauthorized access, use, disclosure, and destruction. It includes the principles and rules that govern the data collection, use, storing, sharing, and processing of the data and has the ability to ensure that the individuals have their own authority of control over their own personal digital information.

They may be developed by governments international organizations, or industry groups to provide the guidelines and standards for data protection and practices. These may vary depends on jurisdiction, industry, and specific requirements of the organization.

These laws, rules and regulations, frameworks and policies are different from country to country although we will dive in to main and more interesting areas in some of them.

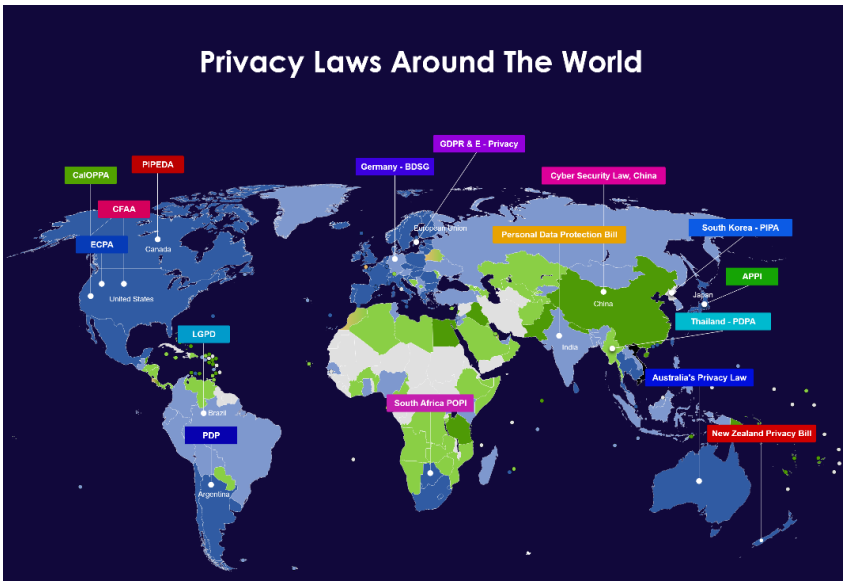

Figure 1: Privacy Laws around the world: Miro.medium.com

3.4.2.1. GDPR (General Data protection Regulation).

A European Union (EU) rule known as the General Data Protection Regulation (GDPR) went into force on May 25, 2018. Its main objective is to safeguard EU citizens' personal information and privacy. Regardless of where an organization is located, it must comply with the regulation if it processes the personal data of EU citizens. This covers companies, agencies, and nonprofits that handle any kind of personal data [4].

The GDPR provides a framework for how organizations should collect, process, store, and protect personal data. It gives individuals more control over their data and requires organizations to provide clear and concise privacy policies. Failure to comply with GDPR can result in significant fines, up to €20 million or 4% of global annual revenue. Overall, the GDPR has increased privacy protections for individuals in the EU and raised awareness of the importance of data protection globally.

3.4.2.2. California Privacy Rights Act (CPRA).

This was passed in November 2020 and into effective on January 1, 2023. It builds on the California Consumer Privacy Act (CCPA) and gives residents of California additional privacy rights, such as the ability to stop companies from disclosing their personal information, the ability to correct inaccurate personal information, and the ability to restrict the use of sensitive personal information. The California private Protection Agency, which will be in charge of upholding the legislation and defending the private rights of Californians, is another new enforcement body established under the CPRA.

3.4.2.3. California Consumer Privacy Act (CCPA).

A data privacy regulation known as the California Consumer Privacy Act (CCPA) became operative on January 1st, 2020. It gives residents of California a number of rights regarding their personal information, including the right to know what data companies are gathering about them, the right to ask that companies delete their data, and the right to refuse to have their data sold. Businesses that fit specified requirements and have clients in California are subject to the CCPA. A violation of the CCPA may result in hefty fines and judicial action.

These both regulations are having effect on US citizens as well the service and product users of the state companies.

3.4.2.4. Convention 108.

This is a convention opened by the council of Europe which collect signatures on 28th January 1981 and was the first legally blinding international in the data protection field [6]. Under this, the parties are required to take the necessary steps in their domestic legislation to apply the principles to make sure they respect in their boundaries for fundamental human rights of all individuals with regard to persons data processing.

3.4.2.5. Personal Data Protection Act.

The Personal Data Protection Act (PDPA)is a data protection law that governs the collection, use, and disclosure of personal data by organizations which used in countries like Singapore and Sri Lanka. The PDPA establishes rules on how personal data should be collected, used, and disclosed, and it requires organizations to obtain consent before collecting, using, or disclosing personal data. The PDPA also provides individuals with the right to access and correct their personal data held by organizations.

3.4.3. Policies and practices.

In the data protection these regulations the policies and practices are related with frameworks in which mostly they are tailed for specific needs of the organizations. They also take a part ensuring the data privacy security. Some of the common policies and practices included in frameworks are:

- Data minimization.

  Collection and processing of the information are only for the specific purposes and limiting the use of personal information to that purpose. Using the data minimization there will be fewer bulk data that the organizations have to put their concern about.

- Consent.

  This involves obtaining clear and informed consent from the individuals before the collection, using and sharing of their digital data like the privacy policies and terms. Consent should be given freely, specific, and revocable at any time.

- Security.

  Implementing an appropriate security measure on protecting data, ensuring that no unauthorized access, use or disclosure or destruction. Giving the Proper security measures are the objective in this.

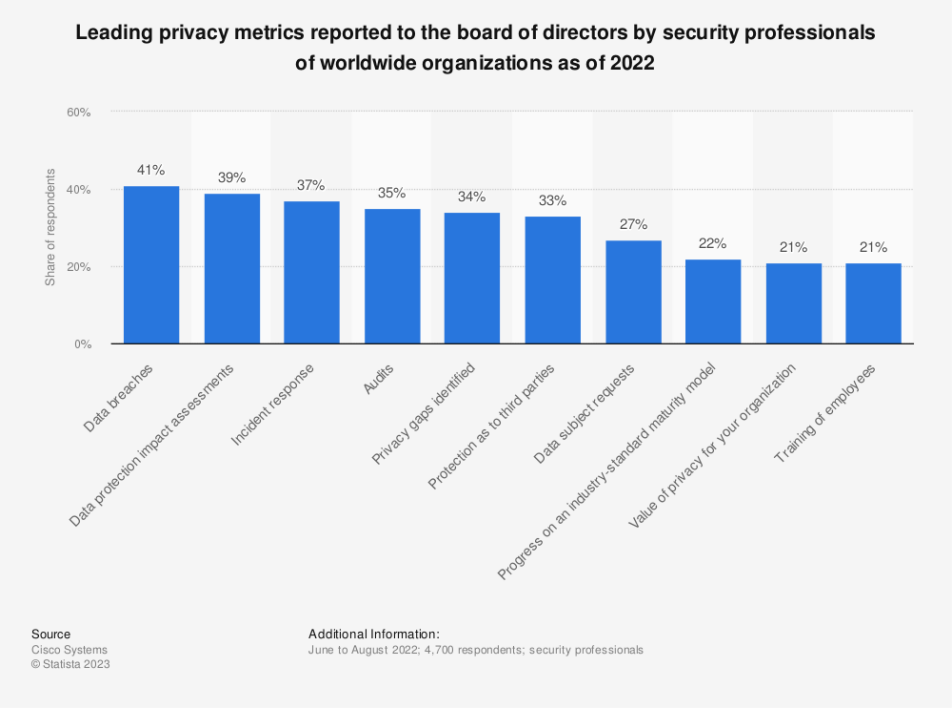

Figure 2:Leading privacy metrics reported to the board of directors by security professionals of worldwide organizations as of 2022.

- Training and awareness.

  Giving the training, awareness and proper knowledge to the users, employees and contractors or third-party service providers on data protection policies and practices. This makes sure the less of the human mistakes.

- Data breach responses.

  This includes the Detecting, investigating, and responding to data breaches are more established in this. Including the notifying the affected individual and regulatory authorities as required by law.

3.5. Data breaches and Impact of data breaches.

Data breaches can lead to identity theft, fraud, and other privacy violations, which can be used to commit crimes, access financial accounts, and compromise an individual's reputation.

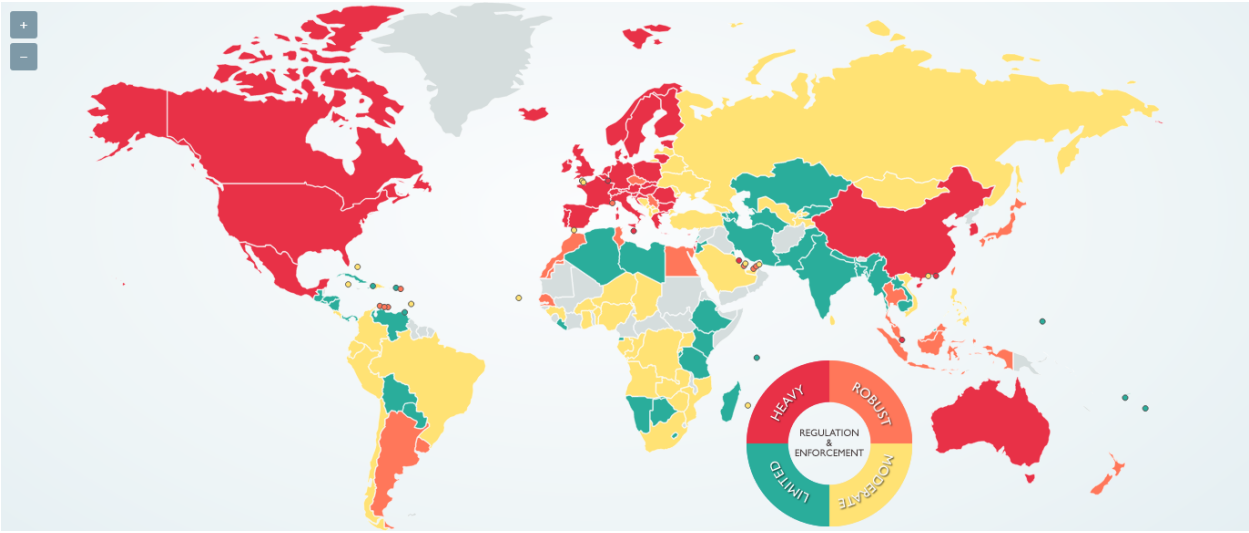

Figure 3: Compare data protection laws around the world: dlapiperdataprotection.com.

Data breaches can also have a major impact on businesses side. The loss of confidential data can lead to financial losses, damage to a company's reputation. Companies may also face regulatory fines and penalties for failing to protect personal information and comply with data privacy regulations.

3.6. Data privacy on International Trade.

Data privacy protection policy proposals are constantly evolving, and there is no agreed-upon menu of data protection options, which comes to the challenges in international trade like balancing the need for data protection with the free flow of data. Many countries have their own data privacy laws and regulations, which make it difficult for businesses to navigate the complex web of regulations and comply with the thousands of rules.

To address these challenges, there have been efforts to develop international standards for data privacy. The General Data Protection Regulation (GDPR) is a key example of such a standard, providing a complex framework for data protection across the European Union. The GDPR has set a high bar for data privacy regulations and has been influential in shaping data protection laws in other countries like Sri Lanka, India, Brazil, Japan, and Even the US [7]. In the end greater cooperations among countries is needed to develop consistent data privacy regulations to mitigate these challenges.

3.7. Current state of data privacy regulations.

The current state of data privacy regulations varies significantly around the world. Some countries have comprehensive data privacy laws and regulations, while others have more limited or no data privacy protections in place**.**

European Union, the General Data Protection Regulation (GDPR) has been in effect since May 2018. The GDPR provides a comprehensive framework for data protection, giving individuals greater control over their personal data and imposing significant obligations on businesses that process personal data. The GDPR has been influential in shaping data privacy regulations around the world, with many countries adopting similar laws and regulations.

In the United States, data privacy regulations are currently less comprehensive than in the EU, with a patchwork of state and federal laws governing data privacy. The California Consumer Privacy Act (CCPA), which went into effect in January 2020, provides some data privacy protections for California residents, but there is currently no federal data privacy law in place.

4. Future of the Data Privacy Rules.

4.1.Increased global harmonization.

Globally, the increasing number of data privacy laws and regulations, most which are formed around on GDPR. Which global companies needed to adapt to their compliances with a wide variety of laws, with depending on where they will operate. Such as, SOFIPO in Mexico, Updated Data privacy act in Australia, PIPL in China, LGPD in Brazil, Amended PDPA in Singapore, and DCIA in Canada. In US [8].

4.2.Expanded rights for individuals.

Expanding individuals' rights to control their personal data, like right to access, right to erasure, the right to object to processing, the right to data portability, and the right to be informed. Even they give more control over their personal information, implementing them can be challenging for businesses and organizations. These regulations reflect a growing recognition of privacy's importance in the digital age and are a positive development for individuals. The California Consumer Privacy Act (CCPA), which grants Californians the right to know what personally identifiable information is being collected about them and the ability to ask that it be destroyed, is one example.

4.3.Greater emphasis on privacy by design.

Businesses and organizations must consider data privacy from the beginning of the design process for their products and services due to the evolution. This approach involves identifying and addressing potential privacy risks and implementing privacy-enhancing measures at every stage of the product or service's development. Businesses and organizations can prevent data privacy from being added as an afterthought to their products and services by adopting privacy by design. This strategy guarantees that privacy is taken seriously throughout the company and helps to increase consumer trust.

4.4.More stringent enforcement mechanisms.

Regulations governing data privacy are getting stricter and enforcement is getting stronger. One example of this is the European Data Protection Board's recent decision to issue a €225 million fine to WhatsApp for violating the General Data Protection Regulation. The EDPB found that WhatsApp did not provide adequate transparency around how it processed users' personal data and did not obtain valid consent from its users. Another example is the California Privacy Rights Act, which was recently passed and will come into effect in 2023. The CPRA strengthens and expands upon the existing California Consumer Privacy Act and includes provisions such as the creation of a new data protection agency and the ability for consumers to opt-out of the sharing of their personal information. These examples show that

regulators are taking data privacy seriously and are willing to take strong enforcement action against companies that do not comply with data privacy regulations.

4.5. Changes to Ad-funded Products.

Technology and IT companies That handles the Sensitive data will continue to make changes to their provided services and products in reaction to growing awareness and regulation of data privacy. Examples like Apple which they ensures the guarantee of the data privacy as their part of their valuable proposition. [8] For Companies like Facebook, Google and Amazon their dependency on the data-driven advertising for gains required a balanced process between their consumers trust while ensuring the ongoing viability of their advertising businesses [8].

4.6. More Businesses Prioritize Privacy and Data Protection.

As more organizations realize how important it is to protect customer information, a trend of businesses prioritizing privacy and data protection is spreading. Cisco and Mastercard are two examples of companies that have made privacy a top priority. Numerous privacy features, including end-to-end encryption for Webex meetings and the capacity to prevent unauthorized access to sensitive information, have been incorporated by Cisco into its products. With its CEO Ajay Banga proclaiming that "privacy is the new gold" and the corporation introducing additional privacy controls in its products to safeguard the personal information of its customers, Mastercard has likewise prioritized privacy. These instances demonstrate how companies are not just adhering to data privacy laws but also making proactive efforts too.

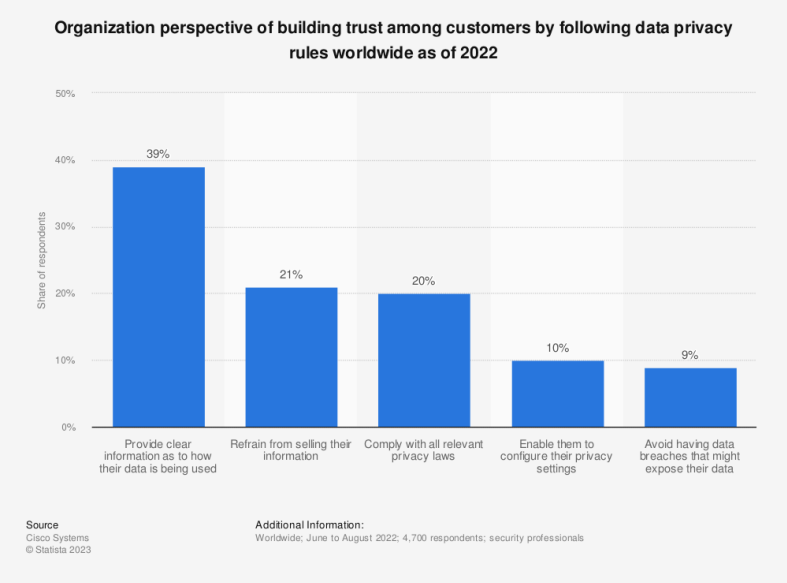

Figure 4: Organization perspective of building trust among customers by following data privacy rules worldwide as of 2022

5. Conclusion

Over time, data privacy rules have evolved significantly to protect individuals' personal information. In older days, privacy laws were fragmented and focused on specific industries or data types. Today, privacy laws are more comprehensive, covering a wider range of data types and industries and emphasizing individual rights to control their data. For example, data privacy laws like the GDPR and CCPA provide individuals with greater control over their personal data, including the right to access, correct, and delete their data. These laws also hold companies accountable for data breaches and non-compliance with strict penalties.

Data ownership is also a significant aspect of privacy laws. Enforcement of data privacy regulations is becoming increasingly stringent, with significant fines for non-compliance. Interactions between different privacy laws are also becoming more important, especially as data is increasingly transferred across borders.

Looking towards the future, we can expect increased global harmonization of privacy laws, expanded rights for individuals, greater emphasis on privacy by design, more stringent enforcement mechanisms, and changes to ad-funded products. For example, the California Privacy Rights Act expands upon by providing additional rights for Californians, such as the right to restrict the sharing of their data.

Privacy by design is becoming increasingly important, with companies building privacy into products and services from the ground up. Apple's Intelligent Tracking Prevention technology is an example of this approach, as it prevents advertisers from tracking users across the web without their consent.

Changes to ad-funded products are as advertisers seek to comply with privacy regulations while still delivering personalized advertising. Contextual advertising, where ads are targeted based on the content of a webpage rather than the user's personal information, is becoming more popular.

In conclusion, the laws governing data privacy have changed dramatically throughout time and will do so in the future. Individuals' rights to manage their personal data are receiving more attention, and increasing enforcement of privacy laws is anticipated. As businesses attempt to strike a compromise between privacy concerns and the demand for tailored advertising, privacy by design and adjustments to ad-funded goods are also expected.

6. References.

[1] C. Véliz, Privacy is Power: Why and How You Should Take Back Control of Your Data, Transworld, 2020.

[2] P. M. S. &. K.-N. Peifer, "Structuring International Data Privacy Law".

[3] C. C. C. Kevin M. Alvero, "Data Ownership: Considerations for Risk Management," April 2020.

[4] E. Union, "General Data Protection Regulation (GDPR)," 2018.

[5] C. R. Service, "Data Protection and Privacy Law: An Introduction," 2022 Updated.

[6] C. o. Europe, "Convention108-and-Protocol".

[7] D. P. Intelligence, "DLA piper Data Protection Handbook," DLA Piper Intelligence.

[8] R. Andruss, "A Brief History of Data Privacy, and What Lies Ahead," 2022.