Data Privacy and Cybersecurity

Kamshad Mohsin[1]

Introduction

Data privacy refers to the protection of personal information and data from unauthorized access, use, disclosure, disruption, modification, or destruction.[2] This can include things like ensuring that personal information is only collected and used for legitimate and authorized purposes, providing individuals with control over their personal data, and protecting personal information from being accessed or disclosed without permission. Data privacy also involves ensuring that personal data is accurate, complete, and up-to-date, and that it is properly stored and handled in a secure manner.[3] Cybersecurity is a subset of data privacy that focuses on protecting data and information from unauthorized access or attacks by hackers or malicious software.[4] This can include things like implementing strong password policies, using encryption to protect data in transit and at rest, regularly updating and patching software to fix security vulnerabilities, and using firewalls and other security measures to prevent unauthorized access to networks and systems. Cybersecurity also involves monitoring for potential security threats and responding quickly to any incidents that do occur in order to minimize their impact.[5] Both data privacy and cybersecurity are important for ensuring the security and integrity of information and personal data in the digital age.[6]

Is Data privacy and cybersecurity essential?

In today's world, where so much of our personal and sensitive information is stored and transmitted digitally, this includes things like financial information, medical records, personal identification information, and other sensitive data.[7] This information is often stored on computers, smartphones, and other devices, as well as on servers and in the cloud. This makes

[1] Assistant Professor, Maharishi University of Information Technology

[2] Bigelow, S. J. (2022). *data privacy (information privacy)*. CIO; TechTarget. https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy

[3] *Data protection and privacy laws | Identification for Development*. (2016). Worldbank.org. https://id4d.worldbank.org/guide/data-protection-and-privacy-laws

[4] Kaspersky. (2022, May 16). *What is Cyber Security?* Www.kaspersky.co.in. https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security

[5] *The Five Functions | NIST*. (2018, April 12). NIST. https://www.nist.gov/cyberframework/online-learning/five-functions

[6] Khan, A. (2022, November 28). *The Importance of Data Security in 2022*. Intellipaat Blog; Intellipaat. https://intellipaat.com/blog/importance-of-data-security/

[7] Nass, S. J., Levit, L. A., Gostin, L. O., & US), M. (2021). *The Value and Importance of Health Information Privacy*. Nih.gov; National Academies Press (US). https://www.ncbi.nlm.nih.gov/books/NBK9579/

it essential to have strong data privacy and cybersecurity measures in place to protect this information from unauthorized access or attacks. It is important to have measures in place to protect that information from unauthorized access or attacks. Data privacy and cybersecurity are essential for maintaining the confidentiality, availability, and integrity of data and ensuring that individuals' personal information is protected.[8] This can include things like encrypting data, implementing strong password policies, and regularly updating security measures to stay ahead of potential threats.

Data privacy Laws

Data privacy laws are laws that regulate the collection, use, disclosure, and protection of personal information and data.[9] These laws are intended to protect individuals' personal information and ensure that it is only collected, used, and disclosed for legitimate and authorized purposes. Data privacy laws can vary depending on the country or region, but many of them have similar requirements and principles. For example, many data privacy laws require companies and organizations to obtain individuals' consent before collecting their personal data, to provide individuals with control over their personal data, and to ensure that personal data is handled and stored securely.[10] This can include things like giving individuals the right to access their personal data, the right to correct any errors or inaccuracies in their personal data, and the right to request that their personal data be deleted. Data privacy laws also typically require companies and organizations to be transparent about how they collect, use, and disclose personal data, and to provide individuals with clear and easy-to-understand information about their data privacy rights and choices.

Some common examples of data privacy laws include the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States.[11]

General Data Protection Regulation (GDPR)

[8] Gil, A. (2018, September 25). *Data Security - Confidentiality, Integrity & Availability | kVA*. KVA by UL. https://www.kvausa.com/data-security-confidentiality-integrity-and-availability/

[9] Staff, O. (2022, July 4). *Data privacy laws: What you need to know in 2022*. Osano; Osano, Inc. https://www.osano.com/articles/data-privacy-laws

[10] Legal, PrivacyPolicies. com. (2018, February 6). *What's Data Privacy Law In Your Country?* Privacy Policies; PrivacyPolicies.com. https://www.privacypolicies.com/blog/privacy-law-by-country/

[11] Kucera, D. (2022, January 18). *CCPA vs. GDPR: Similarities and Differences Explained*. Okta.com; Okta Inc. https://www.okta.com/blog/2021/04/ccpa-vs-gdpr/

The General Data Protection Regulation (GDPR) is a data privacy law that was adopted by the European Union (EU) in 2018. It establishes a set of rules and requirements for the collection, use, and protection of personal data of individuals in the EU.[12] Some of the key provisions of the GDPR include:

- The requirement for companies and organizations to obtain individuals' consent before collecting their personal data, and to provide clear and easy-to-understand information about how their personal data will be used.
- The right of individuals to access their personal data, to request that their personal data be corrected or deleted, and to object to the processing of their personal data.
- The requirement for companies and organizations to implement appropriate technical and organizational measures to protect personal data against unauthorized access, use, disclosure, or destruction.
- The requirement for companies and organizations to notify individuals and the relevant authorities of any personal data breaches that occur.
- The imposition of significant fines and penalties for companies and organizations that fail to comply with the GDPR's requirements.

Overall, the GDPR is intended to give individuals greater control over their personal data and to ensure that companies and organizations handle personal data in a responsible and transparent manner.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) is a data privacy law that was passed in the state of California in 2018. It applies to businesses that collect personal information of California residents and that meet certain criteria, such as having annual gross revenues over $25 million, buying or selling the personal information of more than 50,000 consumers, households, or devices per year, or deriving more than 50% of their annual revenues from selling consumers' personal information.[13] Some of the key provisions of the CCPA include:

- The requirement for businesses to disclose to consumers what personal information they collect, how they use it, and with whom they share it.

[12] *EU General Data Protection Regulation (GDPR) - Definition - Trend Micro IN*. (2018). Trendmicro.com. https://www.trendmicro.com/vinfo/in/security/definition/eu-general-data-protection-regulation-gdpr#:~:text=What%20is%20the%20EU%20General,which%20was%20adopted%20in%201995.

[13] *California Consumer Privacy Act (CCPA)*. (2018, October 15). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

- The right of consumers to opt out of the sale of their personal information.
- The right of consumers to request that businesses delete their personal information.
- The requirement for businesses to implement reasonable security measures to protect consumers' personal information.
- The imposition of significant fines and penalties for businesses that fail to comply with the CCPA's requirements.

Overall, the CCPA is intended to give consumers greater control over their personal information and to hold businesses accountable for their handling of personal data.

Personal Data Protection Bill, 2019

In India, there is no specific data privacy law, Personal Data Protection Bill, 2019 is currently under consideration by the Indian parliament, but has not yet been passed into law.[14] Once passed, it will establish a set of rules and requirements for the collection, use, and protection of personal data of individuals in India.[15] Some of the key provisions of the Personal Data Protection Bill, 2019 include:

- The requirement for companies and organizations to obtain individuals' consent before collecting their personal data, and to provide clear and easy-to-understand information about how their personal data will be used.
- The right of individuals to access their personal data, to request that their personal data be corrected or deleted, and to object to the processing of their personal data.
- The requirement for companies and organizations to implement appropriate technical and organizational measures to protect personal data against unauthorized access, use, disclosure, or destruction.
- The requirement for companies and organizations to notify individuals and the relevant authorities of any personal data breaches that occur.
- The imposition of significant fines and penalties for companies and organizations that fail to comply with the Personal Data Protection Bill's requirements.

[14] Krishna Veera Vanamali. (2022, August 5). *Why does India not have a data protection bill yet?* @Bsindia. https://www.business-standard.com/podcast/economy-policy/why-does-india-not-have-a-data-protection-bill-yet-122080500071_1.html

[15] *The Legal 500*. (2019). Legal500.com. https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/

Overall, the Personal Data Protection Bill, 2019 is intended to give individuals greater control over their personal data and to ensure that companies and organizations handle personal data in a responsible and transparent manner.

Cybersecurity Laws and regulations that aim to ensure data privacy

There are many different cybersecurity laws and regulations that aim to ensure data privacy. These laws and regulations can vary depending on the country or region, but many of them have similar provisions and requirements.[16] Some common examples of cybersecurity laws and regulations that aim to ensure data privacy include:

- The General Data Protection Regulation (GDPR) in the European Union, which establishes a set of rules for the collection, use, and protection of personal data of individuals in the EU.
- The California Consumer Privacy Act (CCPA) in the United States, which applies to businesses that collect personal information of California residents and that meet certain criteria, and gives consumers greater control over their personal information.
- The Personal Data Protection Bill, 2019 in India, which is currently under consideration by the Indian parliament and would establish a set of rules for the collection, use, and protection of personal data of individuals in India.

These laws and regulations typically require companies and organizations to obtain individuals' consent before collecting their personal data, to provide individuals with control over their personal data, and to implement appropriate technical and organizational measures to protect personal data against unauthorized access, use, disclosure, or destruction.[17] They also often impose significant fines and penalties for companies and organizations that fail to comply with their requirements.

Conclusion

There are several ways that companies and organizations can ensure data privacy through cybersecurity. Some key steps that can be taken to protect personal data and ensure data privacy include:

---

[16] *Cybersecurity and Privacy Laws Directory*. (2016). Itgovernanceusa.com. https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws

[17] *Data Protection and Privacy: 12 Ways to Protect User Data*. (2022, June 20). Cloudian. https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

- Obtaining individuals' consent before collecting their personal data, and providing clear and easy-to-understand information about how their personal data will be used.
- Giving individuals control over their personal data, such as the right to access, correct, or delete their personal data, and the right to object to the processing of their personal data.
- Implementing appropriate technical and organizational measures to protect personal data against unauthorized access, use, disclosure, or destruction. This can include things like encrypting personal data, using strong passwords, regularly updating and patching software, and using firewalls and other security measures to prevent unauthorized access to networks and systems.
- Monitoring for potential security threats and responding quickly to any incidents that do occur, in order to minimize their impact. This can include things like conducting regular security audits, monitoring for suspicious activity, and implementing incident response plans to handle any security breaches that do occur.
- Providing training and education to employees on data privacy and cybersecurity best practices, in order to help them understand their role in protecting personal data and preventing security incidents.

Overall, ensuring data privacy through cybersecurity involves a combination of technical measures, organizational policies, and employee education and awareness in order to protect personal data and prevent unauthorized access or attacks.