

An Analysis about Different Steps that Play an Indispensable Role in Developing Enterprise Data Protection Framework

Dr Komarasamy G^{1*}, B.Mahesh²

¹ VIT Bhopal University, India

² Associate Professor, Dr.K.V.Subba Reddy Institute of Technology, India

*Corresponding Author Email: gkomarasamy@gmail.com

Abstract

Enterprise data framework is the way of protecting various data or information in a systematic way. This is depicted strategic application in the way of major ethical practices in the company. The EDM structure of the company and this maintain data protection with various steps like, data identification, assigned compliance, tackling of different limitations, creation of report and sensitive data description. Researcher uses "interpretivism" research philosophy and "inductive" research approach to maintain proper strategy and process of work. Secondary data are collected by researcher with help of this qualitative research type. Several types of strategies related to data privacy protection are mentioned in this study. Financial and organisational losses are managed with help of this data protection framework. Authorisation and authentication are two types of data privacy processes globally. Data protection framework is also managed with the help of this privacy framework. 4 P's of data privacy is also mentioned in this study. Security and compliance strategy is also mentioned here. Security threats and privacy threats are mentioned in this study.

Keywords

Data Privacy, Data Protection, Data Protection.

INTRODUCTION

A framework that can handle data or information of any company in a strategic way to keep secure information about many assets is considered to be the enterprise data framework. EDM structure of the company enhances usability of data, maintains reliability of the entire data set and also detects any problem related to data handling. There are mainly five steps to form an enterprise data framework which are: identification of business data owners, controlling the assigned compliance, making a report to the board, tackling different limitations and description of sensitive data elements [1]. "SDE (Sensitive data elements)" are the elements that assure verification of persons with fingerprints, contact information of customers and security numbers or checking of employee backgrounds.

Data sensitivity can be described with the application of taxonomy that can pick assets to apply in the processing activity. The SDE is mainly divided into several types such as: integrity, consent, confidentiality and availability [2]. Confidence is considered to be the maintenance of risk factors and keeping data secret without any disclosure. Availability is considered to be the timely accessible data that needs to be more informative that can maintain advanced development of that company. Consent is the legal requirement that can impact a company as there is a rule to maintain all information of customers to have potential development [3]. On the other hand, integrity is defined as the tolerable activity of the informative section which may

have chance to chance or be lost completely.

This study is aimed at the description of analysis about different steps that play an indispensable role in developing enterprise data protection framework. In this concern, the steps on developing enterprise data protection framework are mainly formed an indispensable role in the organizational sector. The data protection is mainly based on clear knowledge of various technologies which can particularly be maintained by the main company. Data protection should be required in the company which makes protection in the entire organizational system. "Data protection officer (DPO)" has main value in the major business applications which need to ensure clearance of any issues related to data maintenance [4]. There should be pursuing a set of action to sustain privacy of a company which has initiated new regulation. The involvement of right identification of owners can mitigate any issues of data processing.

MATERIALS AND METHODS

Overall strategy of a research work is maintained properly with help of this methodology chapter. Specific procedures are used to identify, select, analyse and process information related to a topic. Methodology section allows evaluating a topic in an organised manner. Several types of experimental values are also collected with help of these methods. Research design helps to maintain analytical approach of a study. Coherent and logical way of research work is also managed by this research design. In this study, "cross sectional" research design is used to maintain proper strategy

of this work. Several types of research problems are faced by researcher, these problems are totally mitigated by this particular research design.

Research philosophy refers to belief of a specific way to collect in depth knowledge and information related to this topic. Assumptions related to a research work are also gathered by researcher by this research philosophy. In this study, “interpretivism” research philosophy is used by researcher to manage a specific role in observing social world. Proper strategy is also used by researcher to finish their research work in a successive manner. “Inductive” research approach is used by researcher to understand specific objectives of this particular study. Secondary data are collected by these individuals with help of qualitative research type. These data are collected from several types of online journals, websites, books and channels. Researcher collects several types of data related to topic from peer reviewed journals which are published after 2019. Authentic and relevant data are also collected by researcher to maintain authenticity of this study.

RESULTS

Data protection framework refers to process of protecting sensitive information's from loss, damage and corruption. A large amount of data is also stored and created with help of this data protection framework. Data protection plays an essential role to maintain business operations. Several types of data are available in a business activity, by which daily progress report of a business activity is gathered properly. Every business activity always tries to maintain data protection methods in a significant way to be up to date [5]. Data protection is one of key challenges of digital transformation in global market. Small amount of data loss creates a negative impact on data protection procedures. Financial and organisational losses are also maintained with help of this data protection process. Sometimes, several types of data related to business activity are totally lost due to lack of data protection. Loss of reputation, customer trust and legal liability is also hampered with help of this data protection. In case a company can easily protect all their data in a significant way, this firm does not face any issue related to data loss.

Data protection strategies mainly focus on three key factors such as: data availability, data security and access control. Accidental damage is also managed with help of this data security method in a simple way. In case a company loses their data related to work process, this company can easily restore all data related to event of damage. Data related to work process is also accessible with help of these protection procedures. Data protection helps to ensure safety and availability of data. Essential key principles of data protection methods are data management and data availability [6]. Several types of data are available in business activity to gather information related to work process. Data management process mainly focuses on two main areas of data protection such as: data lifecycle management,

information lifecycle management. Online and offline storages of essential data are also gathered with help of this data lifecycle management. Context and sensitivity of data is also managed by these data protection methods [7]. In recent days, every industry totally depends upon new and modern technology and the digitisation process.

Several types of data related to business activity are available in global market, data protection method helps to maintain data lifecycle management to gather, analyse and interpret data related to a particular topic. Valuable data is protected in a significant way with help of these data protection procedures [8]. Reporting, analytics, development and testing of business drive data are also maintained with help of this data protection. Information life cycle mainly refers to several types of stages globally such as: collection, processing, use, dissemination, disposition and storage. These five stages are effectively beneficial to protect several types of data related to work strategy. Consistent management of information from creation to final disposition is also managed with help of this information life cycle management globally. Digitalisation process is also helpful for this particular data protection process [9]. Several types of modern technologies such as: data masking, data erasure, hardware-based security and firewalls are used by a company to protect their data on a daily basis.

Unauthorised access of data can easily be maintained with help of this data protection method. These methods are useful for maintaining inappropriate actions with any data. Protection process of data plays an essential role to maintain safety and availability of data. Financial performance of a company is also managed by this data protection procedure. Data protection helps to maintain loyalty and trust of customers globally, by which a company can easily earn high profit from market [10]. Rate of production is also enhanced with help of this data protection process. Competition level is effectively high in global market, for this reason, a company is not capable enough to protect their data related to work. Hence, data security is an essential key factor to maintain overall strategy of work. Initial security layer of data protection method is firewalls. Firewalls are designed to protect data from usage of unauthorised sources [11]. These firewalls work as an intermediary between public and personal internet globally. Pre-configured rules and regulations are also maintained with the help of this firewall. All packets entering and existing a network are inspected by this data protection method.

Several types of firewalls are available in global market such as: circuit-level gateways, tasteful inspection firewalls, application level gateways and next generation firewalls. These tools are effectively beneficial to maintain protection of data related to work on a daily basis. Two processes are used to maintain unauthorised usage of enterprise data. Two types of processes are engaged with data protection such as: authorisation and authentication [12]. Authentication refers to provide proof of authentic users. A secret password, pin and biometric authentication are provided with help of these

data protection methods. Authentication process helps to maintain multi factor authentication globally. Several types of authentication are available such as: behavioural scans, biometric scans, MFA and passwords [13]. In case one user proves their identity and authorisation globally, this particular user can easily access and interact with specific data related to work. Authorising users can easily gain permissions to read, edit and write different sources. Authorisation process also has some examples such as: role based access control, principle of least privilege access and attribute based access control.

Data encryption method converts several types of data into coded form, by which only authentic users can easily understand meaning of those data in a significant way. Risks related to unauthorised users are also mitigated with help of this data encryption process [14]. Security of data is maintained properly by this data protection procedure. Endpoint encryption is also maintained with help of these data protection procedures. Data masking helps to protect data in a successive manner; everyone can not be able to use that data. Only authorised and authentic people can easily use and understand that data. Tokenization is an essential example of data masking. Data with a unique string of characteristics is also replaced with help of these data masking procedures. Data generalisation, data anonymization and data deidentification are suitable examples of data masking process. Hardware-based security is also an essential key factor of this data protection process [15]. Physical protection of software is also managed with help of this data protection process.

Hardware based firewalls and proxy servers are suitable examples of hardware based security. Data backup and resilience helps an organisation to save multiple copies of data. In case a company loses one copy of data, this backup process helps to gather lost data related to work. Redundancy, external hard drives, cloud backup and hardware appliances are included in other types of data backup protection [16]. Data erasure plays an essential role to delete all data related to a topic. These deleted data are not recovered with help of this data erasure process in a significant way. Organisations must be able to destroy all data related to customer's information and also others. For this reason, customer loyalty is enhanced with data erasure process. Customers always try to erase their personal data from company data and this data erasure process can easily maintain this process. Data whipping, overwriting, physical destruction and degaussing are included in these types of data erasure.

A company must follow proper strategy and process of data protection strategy to maintain their work process. Data protection strategy is also needed for each and every company to maintain their profitability and productivity. Some essential pillars are available to robust data protection strategy such as: collect and audit sensitive data, identifying internal and external risks related to data protection, maintaining data protection policy, following a secure strategy and also maintaining compliance strategy [17]. In

order to maintain data protection control, sources, type and storage infrastructures of data are maintained properly with help of this data protection method. Proper strategy must be maintained by a company for protecting their data related to work. Internal and external risks related to data protection process are also measured with help of this data protection process. In case a company identifies their risks related to work, an organisation can easily protect from those risks in a significant way.

Several types of risks are available such as: internal and external risks. Lack of strong passwords, user access management, poor authentication and unrestricted access to storage services and devices are referred to as internal risks. External risks mainly refer to several types of strategies related to social engineering such as: malware distribution, phishing and attacks on corporate infrastructure. Global data protection and privacy rule awareness is also maintained with help of this data protection procedure. Share of internet users is increased on a daily basis by this global data protection. 49% of respondents in Europe were effectively aware of their domestic data protection and privacy rules [18]. This creates a positive impact on the financial performance of Europe. Only 29% of respondents are represented in North America to maintain their data protection process globally. Global data protection should be managed by each and every organisation in global market to enhance their economic growth.

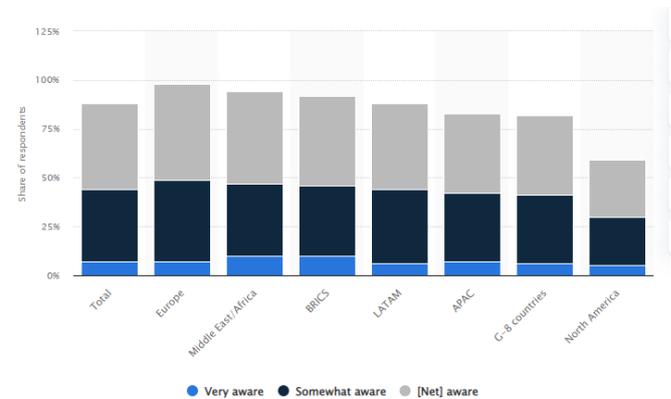


Figure 1: Global data protection and privacy rule awareness

Security strategy related to data is also managed with help of this global data protection procedure. In order to access several types of sensitive data several types of threats are faced by a company to enhance their profitability and productivity [19]. This security strategy helps to reduce those threats from workplace. Issues related to data loss are not faced by those companies in global market. Employees of a company can easily access those data in an organised way, by which these individuals can easily understand work processes and procedures. Employees can easily manage backup's data effectively in a successive manner with help of this security strategy. Security strategy helps to maintain constant data availability within a workplace. Compliance strategy mainly refers to several types of rules and regulations related to data protection. This strategy is effectively beneficial to maintain those norms in a significant way.

Data protection refers to a framework, by which a company can easily understand proper processes for protecting data related to work. In order to protect data, five steps are engaged such as: select proper business data owners, define sensitive data elements, maintain compliance controls, identify risks related to data protection and reporting back to board. Crucial change of data processing methods is to identify suitable data owners. Company management team has a responsibility to organise a data protection program. Critical data are gathered and stored with help of this first step of data protection framework [20]. Sensitive data elements are also beneficial for a company to enhance their performance globally. Taxonomy of sensitive data elements are also maintained by this data protection framework. Several key factors are available to protect data such as: integrity, confidentiality, consent and availability. Several types of information related to data maintain tolerance quality of a company. Several types of data are available for an organisation related to work and customer personal data.

A company always tries to maintain their work process confidentially to mitigate risk factors of unexpected disclosure. Legal information is also managed with help of this data protection framework globally. Several types of challenges are available for maintaining data privacy such as: corporate culture, security threats, cyber security threats and physical security threats. Sometimes corporate culture is not maintained properly due to lack of privacy protection in workplace. Company management team always tries to enhance engagement of several types of employees in workplace. Different employees have several types of mindsets and ideas related to data protection. These individuals can easily provide several new ideas and thoughts for maintaining data privacy. Public and personal information are not managed properly with help of these security threats [21]. Sometimes these issues create a negative impact for maintaining privacy of data related to work. In recent days, everyone uses several types of social media platforms to gather new information. Hence, these cyber security threats are mainly faced by a company for using these social media platforms on a daily basis.

Market size of a company is also enhanced with help of these data privacy methods. Big data market size helps to increase brand value and brand equity of an organisation. Global big data market is forecasted to grow 103 billion US dollars within year of 2027 [22]. This creates a positive impact to maintain financial performance of a company globally. This big market size value is 77 billion US dollars in the year of 2023. Data protection framework of a firm is also enhanced with help of this big data market globally.

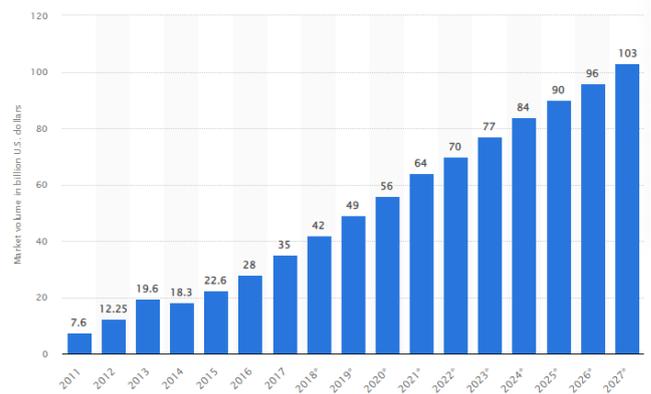


Figure 2: Big data market size revenue

Data privacy plays an essential role to maintain a data protection framework in a significant way. Customers always want to maintain their privacy related to their personal data. In case a company maintains this process, customers are easily attracted by this company globally. Profitability and rate of production of a company is also enhanced with help of engagement of customers. Several types of procedures are also maintained by a company in workplace to manage data protection in a successive manner. In order to maintain identity theft and fraud data privacy framework is an essential tool.

DISCUSSION

Data protection refers to a framework by which a company can easily enhance their customer loyalty in global market. Daily progress reports of a company are also collected with help of this data privacy process. Several types of issues are also faced by a company globally to maintain data privacy protection. Financial and organisational losses are also managed with help of this data privacy protection. In case a company maintains privacy of their public and people's information in the workplace, customers can easily depend upon this particular company in a significant way. Reputation of a company is also hampered due to lack of data privacy protection in market. Data protection framework helps to maintain data protection strategies to enhance their performance in market. Data availability and data privacy is also maintained properly by this particular process of work. In order to create visibility of a data is managed by these data protection strategies globally. Data privacy process helps to maintain process and strategy of work. Internal and external characteristics of a company are known to everyone with help of this data privacy process.

Several types of principles of data privacy are available such as: legitimate, transparency and proportionality. Transparent and flexible workplace is also managed with help of these data privacy procedures. Customers can easily understand quality and quantity of products by this particular process. Three types of privacy are available in global market such as: communication privacy, information privacy and individual privacy. These types should be beneficial for each and every company to maintain a strong customer base.

Customers always try to maintain their privacy. Several types of privacy framework functions are available to manage data protection such as: Govern-P, Control-P, Identify-P, Protect-P and Communicate-P [23]. These principles are effectively beneficial for each and every firm globally. Seven key principles are also engaged with help of data privacy protection such as: accuracy, data minimisation, storage limitations, purpose limitations, integrity, security and accountability. These principles create a positive impact to maintain data privacy procedures.

Physical and digital security is key elements of data security. In recent days, the digitisation process is mainly maintained by a company to maintain data privacy process. Hiring security personnel are also used to maintain the physical security process. In order to maintain a data privacy framework, video surveillance plays an essential role to enhance their profitability and productivity globally. Digital security mainly refers to insisting robust passwords, installing antivirus software and up to date software for this data privacy strategy. Firewalls play an essential role to maintain data privacy procedures. Every company always tries to implement several new technologies and machines in workplace to maintain digital security. Hard drives, files and emails are also managed with help of this digital security procedure. Company has a responsibility to select proper employees in workplace to maintain this privacy protection. Cyber security experts are also needed in an organisation for maintaining operational security.

Experienced and cultured employees are engaged in workplace to maintain data privacy processes. 4 P's of privacy is also maintained by a company globally for maintaining data privacy risks [24]. These 4 P's of privacy mainly refers to places, people, platforms and purposes. Platforms and peoples are key elements of a data privacy framework. Misuse of personal data creates a negative impact on big data privacy risk, by which a company can easily mitigate their issues related to maintaining data privacy.

CONCLUSION

Entire study represented an analysis of different steps that play an indispensable role in developing enterprise data protection framework. Describing this subject, the steps of data protection are mainly described which has been maintained overall description that mainly justifies major subjects. This study insights the importance of data protection which is a major task for a company. In this concern, the data protection office plays a major role that can control major information of the company with application of various regulations to pursue data security. Data identification is the necessary thing that can highlight any issues of data processing. Controlling data is mainly done by DPO who maintain access to various steps to detect any issues related to major data management.

The cross team coordination can be done with the help of major personnel who mainly check various issues related to data protection. The major steps in data protection can

positively play an effective role in a company. Many companies have faced many challenges on data protection which may not be possible due to less activity of DPO or lack of technological usages. Secured data maintenance can bear a sustainable development to adapt new opportunities to way back of unethical practices. Moreover, some fraud cases may lead to huge inefficiency on organizational development which may result in bankruptcy and major threats.

REFERENCES

- [1] Panian, Zeljko. "Some practical experiences in data governance." *World Academy of Science, Engineering and Technology* 62.1 (2010): 939-946..
- [2] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34.1 (2011): 1-11.
- [3] Junlakarn, Siripha, Phimsupha Kokchang, and Kulyos Audomvongseree. "Drivers and Challenges of Peer-to-Peer Energy Trading Development in Thailand." *Energies* 15.3 (2022): 1229..
- [4] Lavrijssen, Saskia, Brenda Espinosa Apráez, and Thijs Ten Caten. "The Legal Complexities of Processing and Protecting Personal Data in the Electricity Sector." *Energies* 15.3 (2022): 1088.
- [5] Mohammed, Ishaq Azhar. "THE INTERACTION BETWEEN ARTIFICIAL INTELLIGENCE AND IDENTITY AND ACCESS MANAGEMENT: AN EMPIRICAL STUDY." *International Journal of Creative Research Thoughts (IJCRT)*, ISSN 2320.2882: 668-671.
- [6] O'Loughlin, Kristen, et al. "Reviewing the data security and privacy policies of mobile apps for depression." *Internet interventions* 15 (2019): 110-115.
- [7] Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. "The European Union general data protection regulation: what it is and what it means." *Information & Communications Technology Law* 28.1 (2019): 65-98.
- [8] Fahey, Robert A., and Airo Hino. "COVID-19, digital privacy, and the social limits on data-focused public health responses." *International Journal of Information Management* 55 (2020): 102181.
- [9] Albrecher, Hansjörg, et al. "Insurance: models, digitalization, and data science." *European Actuarial Journal* 9.2 (2019): 349-360.
- [10] Top, Cemil, and Bayad Jamal Ali. "Customer satisfaction in online meeting platforms: Impact of efficiency, fulfillment, system availability, and privacy." *Amazonia Investiga* 10.38 (2021): 70-81.
- [11] Chakraborty, Partha, Md Zahidur Rahman, and Saifur Rahman. "Building new generation firewall including artificial intelligence." *International Journal of Computer Applications* 975 (2019): 8887.
- [12] Badii, Claudio, et al. "Smart city IoT platform respecting GDPR privacy and security aspects." *IEEE Access* 8 (2020): 23601-23623.
- [13] Campbell, Mark. "Putting the Passe Into Passwords: How Passwordless Technologies Are Reshaping Digital Identity." *Computer* 53.8 (2020): 89-93.
- [14] Di Minin, Enrico, et al. "How to address data privacy concerns when using social media data in conservation science." *Conservation Biology* 35.2 (2021): 437-446.

-
- [15] Kim, Taehyuk, Taek Young Youn, and Dooho Choi. "Deep Neural Networks Based Key Concealment Scheme." *IEEE Access* 8 (2020): 204214-204225.
- [16] Ravi Kumar, M. G. "Network-Attached Storage: Data Storage Applications." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.12 (2021): 2385-2396.
- [17] ACHAR, SANDESH, HRISHITVA PATEL, and SANWAL HUSSAIN. "DATA SECURITY IN CLOUD: A REVIEW." *Asian Journal of Advances in Research* (2022): 76-83.
- [18] Statista Research Department. Share of internet users worldwide who are aware of their country's data protection and privacy rules as of February 2019, by region. Statista. (2022). <https://www.statista.com/statistics/1015291/data-protection-and-privacy-rule-awareness-by-region/>. Accessed 3rd January,2023.
- [19] Wamba-Taguimdje, Serge-Lopez, et al. "Influence of artificial intelligence (AI) on firm performance: the business value of AI-based transformation projects." *Business Process Management Journal* 26.7 (2020): 1893-1924.
- [20] Pirbhulal, Sandeep, et al. "A joint resource-aware and medical data security framework for wearable healthcare systems." *Future Generation Computer Systems* 95 (2019): 382-391.
- [21] Tawalbeh, Lo'ai, et al. "IoT Privacy and security: Challenges and solutions." *Applied Sciences* 10.12 (2020): 4102.
- [22] Taylor, P. Big data market size revenue forecast worldwide from 2011 to 2027. Statista. (2022). <https://www.statista.com/statistics/254266/global-big-data-market-forecast/>. Accessed 3rd January,2023
- [23] ENTERPRISE, IMPROVING PRIVACY THROUGH. "NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0." (2020).
- [24] Dash, Bibhu, Pawankumar Sharma, and Azad Ali. "Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech." *International Journal of Software Engineering & Applications* 13.4 (2022): 1-13.