PalArch's Journal of Archaeology of Egypt / Egyptology

Challenges In Corporate Governance In The Implementation Of GDPR For IT Start-Up Companies In India

[1]*Gaurav Gupta*, [2]*Shaji Joseph*

[1,2] Symbiosis Centre for Information Technology, Pune, India

Gaurav Gupta, Shaji Joseph: Challenges In Corporate Governance In The Implementation Of GDPR For IT Start-Up Companies In India -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x

Keywords: Governance, security standards, Company policies, Internal Audit Team, Employee Awareness training, Information Architecture, organizational structure, data breaches

ABSTRACT

There is a huge growth of start-ups in India, and they have tried to diversify themselves in different businesses. Because of its flat structure, it is difficult for them to enforce the GDPR, and the data processed by it is not covered as mandated by the regulation either due to the high cost of compliance or due to changes in the governance of the company. This research focusses on what are the various challenges Indian IT start-ups face when implementing GDPR on their governance, the reasons Indian start-ups are investing in compliances for these data regulations, information security standard which act as a backbone for the implementation of GDPR and the various aspects of governance in which the IT start-up needs to reform itself. The data gathered for research was through interviews, surveys, and companies' reports. The main findings of the research have shown that Employee awareness training is the most critical obstacle for the start-up and have identified certain information security standards that allow the organization to comply with GDPR.

1. Introduction

Large Companies may rapidly adopt the GDPR, but small and medium-sized businesses are doing the absolute minimum GDPR implementation due to high investment cost. These changes are made to prevent the organization's financial losses and this introduction, in turn, helps to audit their data protection status. Governance, which is the most important aspect for big corporate management, knows its value, so start-ups will look at governance as soon as possible. The company will focus on policies and procedures, decision-making coherence, and transparency. The current architecture of the company is influenced by the introduction of the GDPR, which has a significant effect on the information architecture because there is a strong connection between the information

architecture and IT. Applying the ISO 27001 standard supports the GDPR enforcement process and when implementing the ISO 27001 framework; the organization implements unique data controls and makes them more compliant. One should be prepared to monitor, report, and prosecute personal data breaches and, more importantly, improve data protection in all new ventures and products. Meanwhile, potential businesses will become familiar with this new scenario even if they do not carry out work that falls within the boundary of the GDPR, as data protection and security regulations are becoming more and more stringent around the world. Indian start-ups looking forward to expanding their business in European countries understand the impact of the GDPR and its implementation, and more than 60 percent of Indian firms are unaware of the GDPR implementation, and all non-European firms processing data from European citizens will also have to appoint a member representative in the European Union.

The following objectives will be discussed with the interpretation of the various sources on Corporate governance and GDPR:

Ob1: Description of the different latent variables that have an effect on the corporate governance of the organization in the implementation of GDPR and review of the influence of these variables.

Ob2: Various Challenges to the Corporate governance apart from the latent variables Identified.

Obj3: Identification of various standards that help as the backbone for the implementation of the GDPR.

2. Background

The idea of good governance dates back to the third century B.C. in India and is very old. Where Chanakya (Pataliputra Vazir) carried out the fourfold duties of a king viz. Raksha, Vriddhi, Yogakshema, and Palana. Replacing the King of the State with the CEO of the Company or the Board of Directors, the principles of Corporate Governance refer to protecting shareholder wealth (Raksha), enhancing wealth through proper use of assets (Vriddhi), maintaining wealth through profitable ventures (Palana) and above all safeguarding shareholder interests (Yogakshema or safeguard). Corporate governance was not on Indian Companies' agenda until the early 1990s, and till then nobody would find many references to this topic in the book of the law. In India, structure deficiency such as excessive stock-market transactions, boards of directors without sufficient fiduciary duties, inadequate disclosure procedures, lack of accountability, and systemic capitalism were all crying out for changes and better governance (Poorma, 2019).

Corporate governance has gained significance in India with the introduction of the Companies Act 2013 which, along with the other laws, has put strict provisions on non-compliance. The Companies Act 2013, which replaced on 30 August 2013 the former Companies Act, 1956, and the regulations issued by India's Securities and Exchange Board (SEBI), are the primary sources of the Indian corporate governance regime. The Companies Act stipulations were notified in a phased manner (Ingley et al., 2018). GDPR has no direct

compliance expertise for Indian firms. The EU-based data controllers in their contracts with Indian Data Processors shall be required "to enforce the privacy and security requirements in accordance with the GDPR" and shall also have an "indemnity clause" which shall hold the Indian company responsible for any "loss damages resulting from actions attributable to the Indian firm which may lead to a penalty imposed by the GDPR or the Indian company. In case there is a possibility of any liability on Indian company, the Board has to make an assessment and disclose the risks (*Corporate Governance and GDPR risk | Naavi*, 2018).

Corporate governance and performance in India aren't very strong. This is perhaps because businesses do not observe the rules and regulations very closely during the initial years of the companies. The idea of corporate governance also turns out to be a problem for start-ups, baffling even the stronger ones and the one with creative minds leading those start-ups. In short, corporate governance is the collection of rules and procedures regulating start-ups and dictating how they regulate, administer, and run the organization and its affairs. The primary aim is to objectively and transparently match the interests of the company's investors, executives, staff, and other stakeholders. In your company, higher corporate governance standards are stronger internal checks and balances to prevent mismanagement, conflicts of interest, and abuse of corporate resources. Corporate governance also plays a key role in the public image of a company and is an important factor in evaluating the intrinsic value of the asset. The difficulty that start-ups often face is to build an appropriate corporate governance game plan that fits the maturity level of the start-up. Start-ups prefer to take a "short-term long-term" approach to formulate their business game plan (Opinion | Corporate governance in start-ups, 2018).

Governance and risk specialists, internal audit, and risk management functions are well-positioned to provide the board and management with the inside of the GDPR through assurances. They may help in understanding the various risks of non-compliance that go beyond the potentially significant fines. The value of good corporate governance remains a crucial factor in compliance with the regulations. The GDPR presents major challenges to the organization: Approximately 30 percent of survey respondents cited challenges related to the ambiguity or difficulty of the GDPR, and secondly, they find creativity and analysis. While Data Protection Impact Assessments (DPIAs) are an essential part of the GDPR, there are many comments related to the time it takes to do so. The next challenge is the third party relationship. Supplier agreements were consistently highlighted as requiring considerable time and effort to be revised. It involved the establishment of new contracts where they did not exist or all existing contracts have been reviewed and updated (*GDPR and Corporate Governance the Role of Internal Audit and Risk Management One Year After Implementation Content Map*, 2019).

As companies have limited access to resources at an early stage while holding their shareholders accountable, the best option can be a company structure focused on acquiring resources (Räty et al., 2018). If a start-up is looking to attract investment, governance also comes into play. VCs consider several

factors when evaluating a company. The ability to scale and make money is two of the most important, but it will also contribute to how well the start-up is governed. Governance is such an amorphous activity, but it needs the right culture, policies and procedures, and leadership ultimately. There are steps that a start-up founder should put in place when it comes to creating good governance:

• Identify the culture you want
• Policies and procedures
• Strong leadership
• Transparency in decision-making
• Assign responsibility (Esam, 2017).

Organizations have become more focused on collecting and processing personal data to gain a competitive edge and profit. Consequently, the value of the protection of personal data has increased dramatically, as one of the basic civil rights, the right to privacy, has become more fragile than ever. It is necessary to ensure the process of regular testing, evaluation, and evaluation of the effectiveness of technical and organizational measures after the project implementation of the business with GDPR, to achieve processing security. The GDPR business implementation process is endless, because every new database, every new purpose of personal data processing will need to go through the whole process again, to make the organization 's business fully compliant with GDPR and to reduce the risks of high fines (Todorović et al., 2018). A number of partial compensatory effects, driven by the interaction between specific regulatory requirements and values with the structural features of specific business models, did not have an overall positive or negative impact. There was a certain impact of the legislation. A certain amount of ingenuity and market opportunities have been encouraged by the statute, but it often tends to inhibit certain business models and innovations in ways that policymakers probably did not expect. (Martin et al., 2019).

The GDPR was reviewed, amended, and finally approved by the European Parliament, the European Council and the European Commission in 2015. GDPR came into force in May 2016 and provided the EU member states grace period of two years for the transition to the new law and the establishment of a compliance supervisory body, or the Data Protection Body (DPA). So, in May 2018, GDPR comes into action GDPR aims to increase people's control of their data while simplifying business regulation to ensure that businesses, as well as consumers, benefit from the digital economy. On 14 April 2016, the GDPR was adopted and became enforceable beginning on 25 May 2018. Because the GDPR is just not a regulation, not a directive, it is strictly binding and universal but allows flexibility to be modified by individual member states for certain aspects of the regulation (Team,2017).

With Indian start-ups coming up and working on the new technology like Blockchain, Big Data, Artificial Intelligence, Cloud Computing where a lot of data is processed. GDPR would have a huge effect on the advancement of blockchain technology primarily due to the use of public-key cryptography for most blockchain solutions. Having provided information on GDPR's most

recent developments and legal concepts, the effects of blockchain technology include a first summary of the problems and developments it faces. The right to be forgotten and privacy considerations through design principles are the most prominent challenges for the advancement of blockchain, while opportunities to enhance privacy and improved accountability through immutable process monitoring are often not considered at first sight. Academics and practitioners alike need to keep in mind this changing nature of regulations and technology when conducting research, implementing policies, or developing blockchain solutions. The system needs to be further developed by putting it into practice and by learning from its results (Schwerin, 2018).

GDPR is one of the powerful regulations with serious consequences for cloud providers and businesses interacting with customers. Not only does this legislation have a problem with respect to compliance, but it will also have an impact on the value chain of all industries, including data processors and data controllers' activities. CSPs must update their complete processes, review how their personal information is stored and processed to ensure full compliance which adds value and identify new methods of providing full customer service protection. The study of corporate data management for confidential and sensitive personal data should be started. Different GDPR provisions should be prepared, operational, and technical solutions enforced to address challenges, and policies and procedures should be improved to minimize the worst effects. If both the technical and the organizational solutions are in place, all the provisions of the law can be adapted. With the use of emerging technology such as cloud computing, compliance with the strategy, policy, training, and governance processes needed to comply with GDPR would be expected from a collection of unified responses from the enterprise as a whole (Khan & Gouveia, 2017).

That pervasiveness of technology allows copious amounts of personal data to be obtained, posing threats to the privacy of users and making data security more difficult for organizations. The organization, through the creation of a GDPR privacy mark, will obtain specific consent and disclose its privacy policies to current and future customers (Fox et al., 2018).

The organization that is working on the research are further impacted, according to (Peloquin et al., 2020) It notes that this makes the use of personal data in critical biomedical research more likely to be supported by approaches to ensuring adequate privacy for data subjects. Further clarification from the EDPB will be useful where GDPR has created obstacles for the research community: i) the concept of anonymization, especially whether in some circumstances key-coded information can be used as anonymous; ii) the basis on which personal data can be processed for secondary research purposes; and iii) the basis of the cross-border transfer of the Data. GDPR offers limited administrative compromises to small and medium-sized enterprises; their strategic communication systems, which work with personal consumer data, must meet the regulatory requirements (Kročil et al., 2020).

To communicate with the general public, social enterprises use many approaches. In particular, such services include company websites, online

stores integrated into these websites and social media accounts. Today, social media in particular, is an important form of corporate communication. As both of these techniques operate for personal data, the most recent EU legislation needs to be taken into account by social enterprises. Although the General Data Protection Act provides smaller administrative concessions to small and medium-sized enterprises (SMEs), the marketing communications devices, which operate with personal data for customers, must comply with regulatory requirements. In the Czech Republic, the vast majority of social enterprises use corporate outlets, approximately half of which have a social media profile and one-fifth of which have a social enterprise online store. The new law allows them to adjust their methods of marketing, company, and communication not only for personal data processing but also for their protection (Kuner et al., 2017).

According to (Ponemon Inst., 2012) recent study, After the infringement has been notified, 15 % of the respondents will terminate their relationship and 39% will consider terminating their relationship. 35 percent reported their allegiance and relationships to the company that has no other data infringement. Apart from the loss of customers, another direct economic effect is associated with the risk of a decrease in firm market value following a breach of protection. Accountability includes engagement and clarification of and presentation of compliance by both domestic and foreign stakeholders, legal and ethical responsibilities, strategies, processes, and process, as well as remedying shortcomings. Under Article 5(2) of the GDPR, it is the duty of data controllers to show compliance with data protection laws and regulations (EC GDPR 2016). Improving accountability for an organization improves its ability to respond to security risks and incidents in a timely, effective, and rigorous manner. Many scholars point out that social reporting strategies can produce the "appearance of transparency" without any real effect on the actions and transparency of the company to the individuals concerned. We alert about the possibility of reporting distracting attention from a potentially more efficient means of transparency (Karyda et al., 2016).

Indian start-ups trying to extend their business territories and operating companies need to abide by the various data processing laws and regulations. As European countries strictly abide by the General Data Security Legislation to protect their citizens' collected data. Since Indian start-ups are already struggling with the problems as cash crunch, these GDPR implementations incur additional operational costs, but on the other hand, these standards implementations will benefit large investors, heavy income, and large overseas businesses.One should be prepared for identifying, tracking, and investigating infringements of personal data and, more important, for data protection in all their new projects and products. During the meantime, prospective start-ups will become familiar with this new scenario given their inability to perform research within GDPR because of the growing serenity of data protection and security laws worldwide. A question is needed to start the Data Protection Officer? Initiatives that manage a large amount of information must be accessible to the data protection officer. The regulation would also affect the

way we develop but not much when you're taking blockchain and ICOs (Srivastav, 2018). According to (Suprita,2018) start-ups that operate on data or artificial intelligence need a lot of data-driven decisions to market the goods. The organization needs to ask for the proper consent and the customers will collect the data that is all required. The article also tells about the effect that Indian start-up companies will face who look forward to expanding EU and UK expansion. However, more than 60 percent of Indian companies are still unaware of the new regulation, according to an EY survey.

The big companies were able to implement GDPR easily, but the smaller companies were faced with GDPR implementation problems. The companies must maintain data flow mapping, verifying compliance-based risk. The SMEs has enforced the GDPR policy to the bare minimum to avoid the company's financial losses. Implementation of the GDPR also helps to audit their approach to data security (Sirur, 2018).

3. Identification of Different Latent Variables:

1. *Creation of Internal Audit Team (IAT)*

Boards / CEOs should be invited to encourage the roles and status of internal audit. The internal audit committee should be given clear guidance to strike a balance between compliance and advisory roles. First, a set of widely agreed and applied standards and criteria, while the latter adds value to the company by offering ground-breaking knowledge and enhancement techniques. In order to enhance the role of internal audit in corporate governance, emphasis should be placed on the capacity of internal audits to provide management and board assurance on the integrity of information flows, including monitoring of all internal information-generating systems – internal control, risk identification, and evaluation, management and communication processes, and the provision of information (Leung et al.,2003).

Increased work and a significant amount of time and finances will be required to implement GDPR enforcement strategies in consumer finance companies. Nonetheless, this phase would open up new market opportunities and provide preconditions for the technical modernization of the information system if it was designed and implemented with the right technological solutions, ensuring that further optimization of business processes would eventually boost customer satisfaction. The organization needs to update its business strategy and IT and infrastructural transformation strategy to draw on its potential benefits of GDPR compliance, to define growth and investment goals, and finally to formulate and execute a comprehensive plan to achieve this aim (Tsaneva, 2019).

2. Change in Role and Responsibilities (RRE) and Organizational Structure (OSC) with Implementation of GDPR

The business needs to get ready for the changes in the positions and obligations and their specific delivery with the GDPR being adhered to. Some legally required milestones will improve the company when adopting GDPR. According to GDPR Article 37, the appointment of a Data Protection Officer

(DPO) is important which leads to a change in an organization's structure and roles and responsibilities. The duties and obligations of the DPO in respect to certain positions within the company should be clearly defined within a corporate governance structure. Organizations should consider formally adopting, if not already in place, the Three Lines of Defence model. Article 25 stressing the workplace preparation of the data processing staff (*GDPR and Corporate Governance the Role of Internal Audit and Risk Management One Year After Implementation Content Map*, 2019). Good collaboration exists between information governance and IT governance, using the GDPR implementation example. There is something that needs to be done in Information architecture. The validation of and improvement of the design principles through other information governance tasks should be given greater emphasis (Burmeister et al., 2020).

3. GDPR and Information Security Standards (ISS)

According to the principles of the internal audit department, corporate governance development can only assist in dealing with the GDPR. Compliance with security requirements helps in the GDPR-compliant organization. The ISO 27001 program encourages the implementation of GDPR enforcement in any organization, as it offers access to all risks associated with the business, and the data are high risk. The frequent audits helped to test vulnerabilities associated with the results. The implementation of ISO / IEC 27001 is especially capable of demonstrating compliance with the current GDPR requirements. The new Data Protection Regulation implements a set of rules requiring inspections by organizations. To order to meet these requirements, the introduction of ISO 27001 would benefit organizations. Different requirements may form the basis for GDPR compliance (Lopes et al., 2019).

Although the GDPR has had a positive effect on data protection rights and information integration, its presence within the EU, its primary target area, is more pronounced. Second, while policies are constantly getting longer and covering more topics of privacy, more change is to come before we achieve a stable status of full disclosure and openness. It seemed that the privacy policy was more GDPR focused. The policies which adjust related to the data being stored by the company's retention period. The GDPR is acting as a catalyst for important privacy policies. The general implementation of data privacy rights and information has had a positive impact (Linden et al., 2020).

4. Third-Party Involvement (TPI)

Data controllers may be held liable for third party data breaches resulting from data handling entities. The GDPR poses the question for businesses on how to ensure their activities are based on foreign data processors their compliance with regulations. (Kurtz et al. ,2018) Patterns in third party numbers and types are specific for the groups of websites and countries. Analyzing the number of third parties over time, although we see a reduction in the number of third-

party sites in some categories, we are wary of believing that GDPR will result in fewer external activities (Sørensen et al.,2019).
Average third parties fell by more than 10% after GDPR, but it was found that there was not any decrease in the long-term numbers of third party cookies when analyzing actual browsing history for users over a year, which indicates that users don't take advantage of GDPR's privacy-enhancing options. Also, accepting standard choices would usually end up storing more cookies than on sites that provide a notification of cookies stored but not give users the option of which cookies or which do not provide a warning among websites that offer users a choice of whether and how to track them (Hu et al.,2019).

5. Employee Awareness Training (EAT)

The fulfillment of the GDPR obligation calls for a substantial amount of investment in terms of accounting, human resources, and the preparation of employees. They are not really ready for the changes and may not be aware of future requirements and coercive action by the GDPR (Tikkinen-Piri et al.,2018). According to (Gunasinghe, 2019) shows how customers clearly accept, the customer's correct notification, various customer requests for data access handling, customer requests for deletion of data, and customer data portability requests.
According to the (Macaulay, 2018) article by the Techworld on the leading start-up in the UK to find their preparation for the GDPR implementation. The firm has identified all the data being stored and identified how it is being used. The start-up has been through an internal audit review for all the gaps for each manager and external counsel and its recommendations have driven the organization to change the company procedures and improve data privacy and data security. Speaking about the new duties, a member of each team was chosen to supervise compliance with all data processing. Much effort has been made to teach enforcement bases to the staff. As a matter of policy, all workers must undergo regular training on various topics; data security and improvements within GDPR are a part of that. The organization also says "People who are motivated by their data ownership will expect more from the organizations that represent them. This creates more competition for customers and better results and we like to think we are an organization that can help deliver this shift. So, we 're for it all.

4. Methodology

Questionnaire

The questionnaire was broken down into four sections. The first section consists of the general details of those respondents who will be taking the survey. These details include the organization they belong to and the role they hold in the organization.
The second section contains how much the respondent agrees/disagrees with the selected variables identified from previous research papers that have worked on GDPR implementation challenges in large organizations.

The third segment is a Rank-based query where the respondents rate the latent variables found on a scale of 1 to 7. The fourth section consists of the open-ended questions in which the respondents must provide detailed responses based on their experiences.

The questionnaire was filled out by the respondents who serve as consultants for cybersecurity, data protection officers, or are in the senior management involved in the governance of Start-up in India.

Sampling

The respondent surveyed as part of the research was drawn from the various IT start-ups that have already implemented GDPR or comply with these data regulations. Some of the respondents work as cybersecurity consultants who helped companies achieve GDPR. Some of the respondent's business operates as third-party firms that manage the outsourced work from larger multinational firms that operate in European countries or handle data from European people. The table-1 outlines the demographic details of the respondents from which the data was obtained.

Table 1.Demographic details of respondents

S. No	Business Line	Role	Designation
1	Consultancy firm	Consultant	Consultant
2	Research firm	Data Protection Officer	DPO
3	Consultancy firm	Consultant	Consultant
4	Data Analytics company	Data Protection Officer	DPO
5	Third party solution provider	Head Delivery	Vice President
6	Risk Assessment and Audit firm	Delivery Manager	Asst Vice President
7	Job Application portal	Data Protection Officer	DPO
8	Law related	Start-up owner	Team Leader
9	Software solution provider	Data Protection Officer	DPO
10	Consultancy firm	Consultant	Consultant
11	Mobile application	Delivery manager	AVP
12	Cybersecurity solution provider	Sales & Marketing	Sr. VP Sales & Marketing
13	Consultancy firm	partner	partner
14	Data analysis and report providers	CEO	CEO
15	Software solution provider	Pentester	Information security Engineers

5. Analysis and Discussion

The different variables that have been identified are:

- Employee Awareness Training (EAT)
- Information security Standards (ISS)
- Third-party involvement (TPI)
- Cost of Implementation of GDPR(CIG)
- Internal Audit Team (IAT)
- Roles and Responsibilities of the employee (RRE)
- Organizational Structural Change (OSC)

Based on the statistical analysis of the 5-scale Likert data that has been collected in the second section, the average of all the response per identified variables has been calculated to understand the most important and the least important parameters which act as the challenges for the implementation of the GDPR. These challenges were categorized in different categories on the range of average. The table 2 defines the different categories.

Table 2. Average categorization

S. No	Average Rating Range	Category
1	Greater than 4	Strongly Agree
2	3-4	Partially Agree
3	Less than or equal to 3	Strongly Disagree

Table 3.Categorization of the latent variable based on Response

S. No	Latent Variable	Category	Average Rating value
1	Employee Awareness Training (EAT)	Strongly Agree	4.41
2	Information security Standards (ISS)	Strongly Agree	4.16
3	Third party involvement (TPI)	Strongly Agree	4.08
4	Cost of Implementation of GDPR(CIG)	Partially Agree	3.75
5	Internal Audit Team (IAT)	Partially Agree	3.67
6	Roles and Responsibilities of employee (RRE)	Strongly Disagree	3
7	Organizational Structural Change (OSC)	Strongly Disagree	3

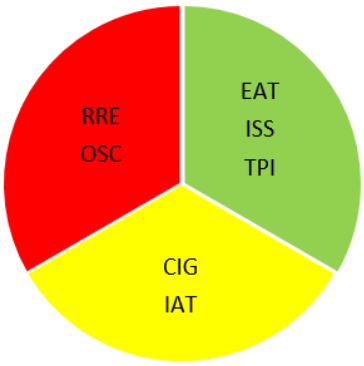

Figure 1. Pie chart representation of the latent variables

It can be clearly understood from table 3 and **Error! Reference source not found.**that many of the respondents firmly agree that employee awareness training, third party participation, and enforcement of the various cybersecurity requirements are the main obstacles in accordance with the GDPR. Changes in the organizational structure and changes in workers 'roles and responsibilities are not so much influenced by any Indian IT start-up companies' compliance with the GDPR. The cost of implementing the regulation and establishing the audit team does not have very significant impact on making organisations complying with GDPR.

To do the thorough analysis, the third section was a Rank based Analysis of the Latent variables identified as the challenges for implementing GDPR. The most important variable was given rank 1 by the respondents while the rank 7 was given to the least import variable.

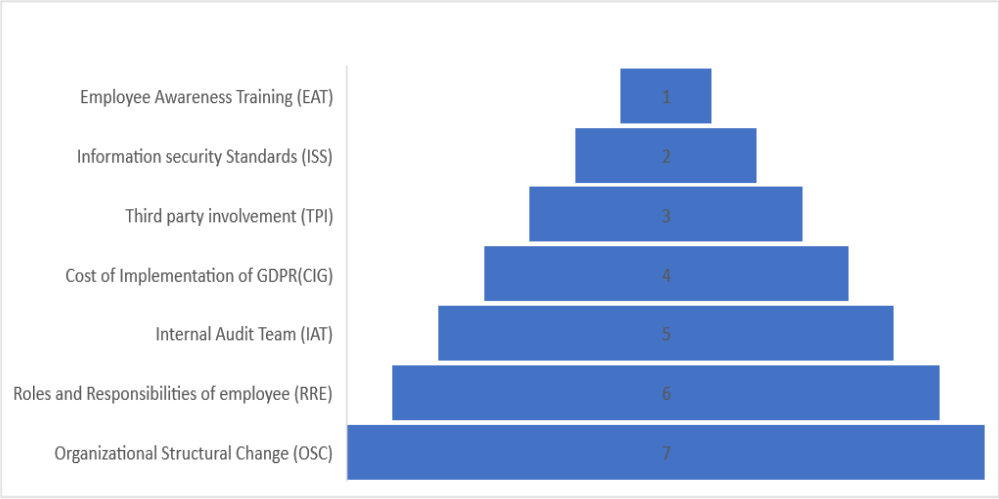

Figure 2.Rank allocation to different variables by respondents

From the Figure 2 it can be concluded that Employee Awareness training is the biggest challenge that the organisation faces where it has been easy for the Indian start-ups to redefine their organisation. The ranking of the different

parameter and the average in the section two concludes the same results of the challenges to the Indian IT start-ups.

Section four of the Questionnaire was having open-ended questions asked from respondents to understand the various challenges apart from the identified can be the major challenges in the implementation of the Data protection regulation. The data were analysed using the grounded theory and then the data was coded using in vivo method. Data that has been collected as part of the open-ended questions where color-coded and bucketed similar ideas into one major category. Under each question, the frequently used words are identified and they are put into the different categories in which they have been identified.

1. The first question asked was what are the different standards which act as a backbone for the implementation of GDPR. The various standards which help as the backbone for the implementation of the GDPR are described in the Figure 3 :

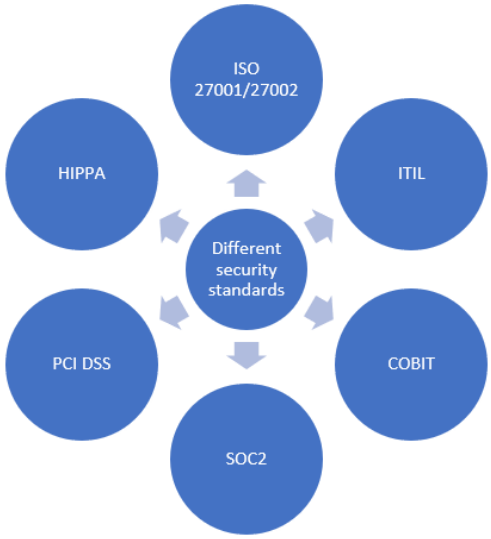

Figure 3.Different security standards

The different standards that the organization implements as the starting point before enforcing the GDPR serve as a bare minimum which can help the organization to be ready for compliance with the GDPR. These standards serve as providing the Information Security Management System (ISMS) requirements. An ISMS is a structured process for safeguarding the organization's sensitive information and controlling the threats to information security. Such principles follow a process-based approach to define, enforce, run, track, manage, and improve ISMS, and it applies irrespective of any international changes that may arise within the organization. These standards also apply to manages the privacy risks.

2. Every company needs to undergo various changes to the organisation's current governance. To understand these changes the respondents were asked about the different adjustments in the organisation's governance. The reported changes are listed in the Figure 4:

Figure 4 Changes in the Governance of the Organisation

With the implementation of GDPR, there is a need to change the different policies that will help the staff to become aware of the standards and to give training. The organisation at the very first need to add the data consent policies in which they need to acquire data subject consents for the processing of their information. After the change in the consent policies there is a need to be change in the data governance policies which provide the proper access rights for the data processing is necessary. A number of changes to the various security policies must be made to prevent any preaching of data that might occur. The security measures should be enforced to secure the data breaches. Not only that but there is some effect on the new Enterprise Architecture which must be made in accordance with the Regulation.

3. Understanding why the Indian Start-up invests in various regulations such as GDPR is very important. The Indian start-ups are investing heavily in making themselves compliant with these requirements for various reasons which has shown in Figure 5**Error! Reference source not found.**.

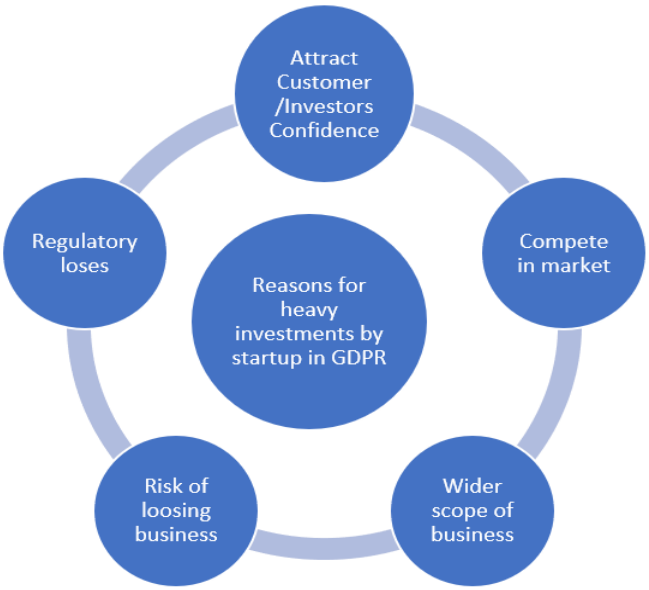

Figure 5 Different reasons for heavy investments of start-ups in GDPR

As the start-up is looking for a lot of investments and customers, customers and investors are increasing these implementations. They can compete easily with competitive firms that lack compliance with these requirements. Because there are different start-ups that lose their business due to various reasons such as large regulatory losses or heavy fines payments, this helps them to avoid any business loss. As these regulations are mandatory for the organizations collecting the European data, this helps them as a wider scope of business for the organizations in these countries if they are compliant.

4. Other challenges identified apart from latent variables, which represent challenges for start-up organizations to implement GDPR are shown in Figure 6**Error! Reference source not found.**.

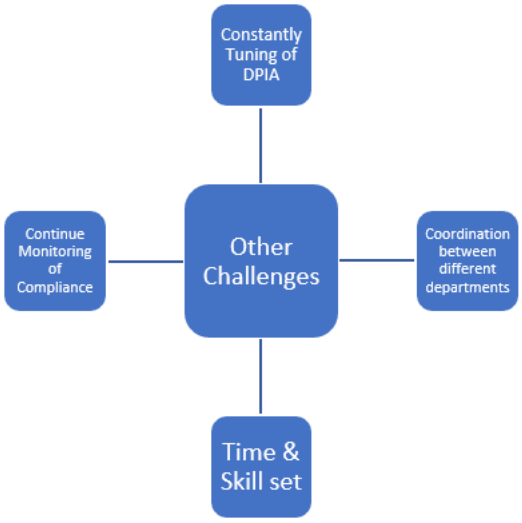

Figure 6 Other Challenges in the implementation of GDPR

The Data Security Impact Assessment (DPIA) is in constant need of turning. A DPIA is a process systematically designed to analyze, identify, and minimize a project or plan's data protection risks. It is a key part of the GDPR 's accountability obligations, and when properly done, it helps you assess and demonstrate how the company fulfills all data protection obligations. Continuous monitoring of GDPR compliance is required as the organization advances as the organization changes. In fact, the application of the GDPR requires a lot of time and expertise. As the organization grows, there is a constant need to communicate with other departments within the business and verify what data they need to process.

6. Conclusion

Indian start-ups seeking to expand their business and seek compliance need to face some challenges, but these challenges are not difficult to overcome if a proper strategy has been put in place that can easily comply with the different aspects of the regulations. It is expected that organizations should review their governance strategy and how they manage data protection as an organizational issue in order to comply with all of the areas listed in this document. The organizational structure of the company and the major changes in the employees' responsibilities and commitments do not pose great challenges. The IT start-up should certainly evaluate after the implementation of the Regulation whether it will gain more profits in terms of future business or retain the confidence of its current clients after the implementation of the Regulation. Any IT company whose primary business deals with the data will consider all of the problems and be prepared. First, they should promote knowledge and design their staff's appropriate awareness training to understand the regulation and how they should handle the data. The organizations at the start can comply with certain international standards of information security that are mandatory for them and can also act as a backbone for the implementation of the GDPR and at the later stage can reduce the financial investment in compliance with the GDPR. All third-party involvement policies need to be redefined, and they should be ensured compliance with the regulations. When the company is ready it needs to redefine the information architecture of the enterprise to ensure proper control of how the data are obtained, stored, processed, and removed. The company would have established an internal audit team for comprehensive auditing of all processes and ensuring that the company follows the Regulations regularly and that any breaches should be reported to the Board of Directors if they have occurred. The existing security protocols and procedures need to be reviewed, and the Senior Management will review the recommendations by the internal audit team and seek to comply with them as early as possible. As the company expands it is the Senior Management's responsibility that they should continually change their DPIA with the guidance of the internal team. Implementing the GDPR raises a range of obstacles for Indian IT companies, but they also make them ready for the relevant data security regulations coming in the future from both Indian and other countries, such as India's PDP Act. Unless the Company already

complies with GDPR, they will not be impacted by the data legislation of any country and the potential effect on their business development. At the board level, the risk of regulatory non-compliance and the cost and organisational effects associated with poor data quality and inaccurate reporting must be addressed, including the selection of a Data Protection Officer at the board level, supervision of internal controls to ensure compliance, analysis by the audit committee and preparation of best practises in the field of corporate objectives

References

Burmeister, F., Huth, D., Drews, P., Schirmer, I., & Matthes, F. (2020*). Enhancing Information Governance with Enterprise Architecture Management : Design Principles Derived from Benefits and Barriers in the GDPR Implementation*. 5593–5602.

Corporate Governance and GDPR risk | Naavi. (.). Retrieved July 11, 2020, from https://www.naavi.org/wp/corporate-governance-and-gdpr-risk/

Esam, A. (2017, March 29). *growthbusiness*. Retrieved from growthbusines: https://www.growthbusiness.co.uk/why-governance-must-be-a-priority-for-startups-2550207/

Fox, G., Tonge, C., Lynn, T., & Mooney, J. (2018). *Communicating compliance: Developing a GDPR privacy label. Americas Conference on Information Systems 2018: Digital Disruption,* AMCIS 2018, 1–5

GDPR and Corporate Governance The Role of Internal Audit and Risk Management One Year After Implementation Content Map. (2019).

Gunasinghe, U., & Khanna, P. (2019). *GDPR employee awareness*.

Hu, X., & Sastry, N. (2019, June). *Characterising Third Party Cookie Usage in the EU after GDPR. In Proceedings of the 10th ACM Conference on Web Science* (pp. 137-141).

Ingley, C., & Wells, P. (2018, October). *GDPR: Governance Implications for Regimes outside the EU. In Proceedings of the European Conference on Management, Leadership & Governance* (pp. 105-113).

Karyda, M., & Mitrou, L. (2016). *Data Breach Notification: Issues and Challenges for Security Management*. In *MCIS* (p. 60).

Khan, S. R., & Gouvia, L. B. (2017). *The implication and challenges of GDPR's on Cloud Computing Industry*. International Journal of Computer Science, 5(7), 106-112.

Kročil, O., & Pospíšil, R. (2020). The Influence of GDPR on Activities of Social Enterprises. *Mobile Networks and Applications*, 1-8.

Kuner, C., Jerker, D., Svantesson, B., Cate, F. H., Lynskey, O., Millard, C., & Loideain, N. N. (2017). The GDPR as a chance to break down borders. International Data Privacy Law, 7(4), 231–2332. https://doi.org/10.1093/idpl/ipx023

Kurtz, C., & Semmann, M. (2018*). Privacy by design to comply with GDPR: a review on third-party data processors.*

Leung, P., Cooper, B. J., & Robertson, P. (2003*). Role of Internal Audit in Corporate Governance & Management, The. Role of Internal Audit in Corporate Governance & Management*, The, viii.

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). *The Privacy Policy Landscape After the GDPR. Proceedings on Privacy Enhancing Technologies*, 2020(1), 47–64. https://doi.org/10.2478/popets-2020-0004

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). *Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. Journal of Information Systems Engineering & Management*, 4(2), 2–9. https://doi.org/10.29333/jisem/5888

Macaulay, T. (2018). *How startups have prepared for GDPR. Retrieved from Techworld*: https://www.techworld.com/data/how-startups-are-preparing-for-gdpr-3668896

Mannhardt, F., Petersen, S. A., & Oliveira, M. F. (2018, June). *Privacy challenges for process mining in human-centered industrial environments. In 2018 14th International Conference on Intelligent Environments* (IE) (pp. 64-71). IEEE.

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). *How data protection regulation affects startup innovation*. *Information systems frontiers*, *21*(6), 1307-1324.

Opinion | Corporate governance in start-ups. (2018). Retrieved July 2, 2020, from https://www.livemint.com/Opinion/HoII4Fmt52VlloPQqY7MnO/Opinion--Corporate-governance-in-startups.html

Peloquin, D., DiMaio, M., Bierer, B., & Barnes, M. (2020). *Disruptive and avoidable: GDPR challenges to secondary research uses of data. European Journal of Human Genetics*. https://doi.org/10.1038/s41431-020-0596-x

Ponemon Institute LLC, (2012), *Consumer Study on Data Breach Notification, June 2012*, available at http://www.experian.com/assets/databreach/brochures/ponemon-notification-study-2012.pdf.

Poorma, V. (2019). *CORPORATE GOVERNANCE IN INDIA- AND*. 6(9), 654–662.

Räty, J. E. (2018). *The role of Corporate Governance in Start-up Companies-Evidence from Finnish equity crowdfunding*.

Schwerin, S. (2018). *Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study. The Journal of the British Blockchain Association*, 1(1), 1–77. https://doi.org/10.31585/jbba-1-1-(4)2018

Sean Sirur, J. R. (2018). *Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In 2nd International Workshop on Multimedia Privacy and Security (MPS '18) at the 25th ACM Conference on Computer and Communications Security (CCS),* (p. 8 pages). New York.

Sørensen, J., & Kosta, S. (2019, May). *Before and after gdpr: The changes in third party presence at public and private european websites.* In The World Wide Web Conference (pp. 1590-1600).

Srivastav, S. (2018). *How Will The EU's New GDPR Affect Indian Startups*? Retrieved July 7, 2020, from https://inc42.com/features/how-will-the-gdpr-affect-indian-startups/

Suprita, A. (2018).*How GDPR Will Affect Indian Startups Processing Data From EU*? Retrieved July 7, 2020, from https://inc42.com/features/how-gdpr-will-affect-indian-startups-processing-data-from-eu/

Team, I. P. (2017*). EU general data protection regulation (GDPR): an implementation and compliance guide. IT Governance Ltd.*

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.

Todorović, I., Komazec, S., Krivokapić, Đ., & Krivokapić, D. (2018). *Project Management in the Implementation of General Data Protection Regulation (GDPR). European Project Management Journal,* 8(1), 55–64. https://doi.org/10.18485/epmj.2018.8.1.7

Tsaneva, M. (2019). *Challenges of GDPR compliance in consumer financing companies*. In Conferences of the department Informatics (No. 1, pp. 103-115). Publishing house Science and Economics Varna.