The role of human resources professionals on the General Data Protection Regulation

PRD Wijesingha[*], HGM Wickremeratne[**]

[*] Faculty of Management Studies, Sabaragamuwa University of Sri Lanka
[**] Faculty of Management and Finance, University of Colombo

DOI: 10.29322/IJSRP.10.08.2020.p10489
http://dx.doi.org/10.29322/IJSRP.10.08.2020.p10489

Abstract- The changes in data protection regulatory impact how we currently manage employee data. Human Resources as a function must know-how companies are faring the impact of this change. What areas companies need to be cognizant of that may open to compliance risks. This study focuses on the issues of individual data privacy breaches and being non-compliant to various data protection regulations in both local and global companies, and human resources responsibility to make it compliant. Though data privacy might apply to many industries, this study gives special reference to the business process management (BPM) industry which is one of the main industries which liaise with data processing and data managing.

Human resource professionals have a major responsibility to make the organization comply with data protection regulations despite the changing roles of human resources. There should be two-way communication between the organization and employees during this journey.

Index Terms- human resource efficiency, human resource professionals' commitment, general data protection regulation

I. Introduction

The world is consistently becoming prone to technological advancements because of globalization which implies organizations to stay up to date to be competitive. Despite being what type of business, you are in, each business has gone through a rapid transformation because of the digitalization. This enables organizations to use advanced enterprise resource planning information systems. In such organizations, all the business functions are centralized and they commonly use shared information. Therefore, information is available at fingertips, and accessing data has never been this easy. According to [2], 81% of the human resource analytics projects were jeopardized by ethical, protection, and privacy concerns. It is needed to ensure data protection and security, especially if it is a cloud, centralized information system.

Security is one of the basic needs of any human being. Especially in the modern digital world, not only physical security but also data security is equally important to all the people. Similar to governments are responsible to ensure the safety and security of the people who are living in a country, Human Resources also responsible to ensure the individual data security of the workplace. Human resource departments use human resource information for their day to day work. Starting from candidate attracting until employees exit or retirement from the company, they have employee personal data in their centralized database. Apart from that, if the company is processing customers' data, there can be sensitive information of the customers such as financial, personal, and legal information which would be highly confidential in nature. Human Resources play a crucial role when it comes to dealing with data security [10]. Sometimes, because of the personality or curiosity for the nature of the data, human resource professionals might try to misuse that data or take advantage of data. At the same time employee may feel insecure about their data privacy, when the human resource department request to provide sensitive data such as family data, past employment data, personal interests, and other sensitive data.

Sensitive data should be managed carefully, as this might be misused by an unknown or unwanted internal or external parties. Organizations may ensure data protection on their sensitive data either ensuring proper employee ethics or establishing a data security policy or being compliant to local or international data protection regulatory bodies [7]. Further organizations may use awareness sessions, training, audits, and different risk matrices to align themselves with required standards. Even though organizations establish precautionary measurements, still there are many incidents of data violations. In case of a data breach, certain regulations will impose exorbitant fines, and amounts will be charged from the company. Not only that, but the organizations may also lose their stakeholders' trustworthiness and credibility, which may lead to loss of employer branding [10].

Though organizations strive to maintain harmonious workplace through policies and

The purpose of this study is to ensure the human resource professionals' commitment towards data protection in Business Process Management (BPM) industry. BPM organizations are all about managing someone else's business process. In this kind of organization, the human resource department is not only responsible to ensure the data protection of their employees but also to make sure their employees safely manage clients' and end-user data.

II. Literature Review

Today's rapidly changing data landscape has led to the necessity for proper data protection on storing, managing, retrieving, and disseminating data from 'good to have' to 'must-have' with utmost importance. Data protection regulations need to ensure

employee data protection for a harmonious workplace [11]. It will make sure the organization is progressing towards the right path establishing the security of such data through proper standards and policies.

Personal data can be defined as "any information that can identify a data subject directly or indirectly, by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural [1]. Further, personal data could be collected only for a specific purpose and not for any other purpose.

Data protection is the process of protecting essential information from corruption, compromise, or loss of data [7]. For instance, the information in which employees hesitate to communicate with third parties such as race or ethnic information, sexual orientation, relationship issues, and political interest [8]. Said information is treated as highly sensitive data where everyone hesitates to share among others. Yet due to information technology, the amount of data gathered and stored is drastically increasing day by day, important to protect those data increases. There are many negative consequences if we fail to protect highly sensitive personal data, including financial losses and poor employer brand. There was a lot of controversy over Facebook and the Cambridge Analytica data breach [3]. Many people have started talking about data privacy and data protection. People have explored what are the actions they could take against the breach of data privacy from the organization's point of view and what are the remedies available for them to seek assistance in such a scenario. Many companies have started updating their company data privacy guidelines and a lot of updates were available for the general public when they access websites of such companies. Identifying the importance of data protection, the European Union (EU) has introduced the General Data Protection Regulation (GDPR) which is one of the most powerful legislatures ever introduced.

The GDPR was introduced to match data protection law across the EU and greatly increases responsibilities on controllers and processors of personal data. GDPR has a significant impact on the use of employee and candidate data in particular and as such, all employers should familiarize themselves with it. GDPR tries to protect data privacy across EU countries and even extended to other countries who are managing or storing data from EU countries with greater obligation and controls [5]. Even a country like Sri Lanka is under such laws if the data processing or controlling of EU countries is done from a Sri Lankan company.

1. The Importance of GDPR Regulations to Sri Lanka

With the increased interest of data privacy in both the local and global contexts, the topic has captured much attention from the general public as well as statutory bodies. Despite being compliant with such different data protection laws, there should be a moral and ethical standard also when it comes to respecting the data privacy of individuals and the right to know of parties whose data are being used for various purposes. Generally, data protection would fall under the function of information technology or information security, whereas because of the nature of the data and policies which should be established across various functions in the organizations, human resources also have to play a critical role to establish the required standards.

Sri Lanka has no legislation in place for data protection and privacy legislation. Though Sri Lanka not introduced any legislative coverage over personal data protection [4] nor has recognized the individual data protection is a fundamental right of Sri Lankan citizens there are certain pieces of statutes support data privacy [4]. This can be considered as a major step towards the protection of data.

2. Human Resource Professional's Commitment to Data Protection

Human resource professionals handle essential human resource tasks such as recruitment, performance management, learning and development, reward management, discipline management, grievance handling, and industrial relations [7]. In BPM organizations, there are separate legal and information technology professionals to ensure data protection. However, the issue of non-compliance to data protection cannot be marked as the sole responsibility of the legal and information technology teams but also the HR professionals carry a lot of weight to ensure there are right actions have been taken to ensure the compliance towards data protection. The compliance is highly challenging to such laws, especially to the laws such as GDPR due to the lack of regulatory support. However, as HR professional there are certain key action should be taken to establish a company with rigid compliance for data protection laws.

Business process management companies are performing outsourcing work for EU countries. If any country works for these countries, it should adhere to data protection regulations. Especially the businesses such as Business Process Management (BPM) and Knowledge Process Management (KPM) who are directly impacted by said law and potentially liable for skyrocketing fines for data breaches. Breach of individual privacy data not only results in exorbitant fines but also to the loss of foreign clients and survival of businesses who are operating in BPM/KPM domains in Sri Lanka. Human resource professionals have access to certain personal data that can be freely available not only for the respective custodians but also to the wider group of people who are in the same department [11]. It is difficult to track who possesses which data if an individual wants to ensure the privacy of their data. Therefore, employees may feel less protection over their data privacy.

Being compliant with data protection regulations would increase the trust and reputation of the organization with the customers and the general public. More awareness and pieces of training on compliance is required to be knowledgeable on the data protection. Increase usage of cybersecurity measures has minimized the threat of data breaches [9]. With increased controls over data protection, certain data access is given to a few individuals even within the human resources department. As the data that the organization holds streamlined, the IT systems may be more effectively used.

Apart from the positive impacts, there are certain negative impacts of data protection regulations on human resources. Human resources would be in great pressure to ensure the safety of the data privacy in the organization at all times without any security breach. Organizations should request for personal data only if it's required and should ensure the removal of such data if not required. When I am conducting interviews with human resource

professionals in the industry, the majority mentions that there is no deletion of personal records from the company. It will remain with the company for a longer period they exit from the company. Which is a controversy for the GDPR? Further, it is always good to have explicit consent from the parties who are shared the data. Seeking specific consent from employers might place human resources in additional pressure on human resources [10]. On the other hand, employees are also under pressure to make sure that personal data are accurate and report if there is a breach within 72 hours [6]. Data protection processes should be designed and shared throughout the organization. Data protection by design ensures that knowledgeable employees are given the task to process personal data [6].

The employees who are processing data should be supported with the right tools and software which will ensure the data integrity in the organization. The cost of such investments would be comparatively higher. In case of any breach in data protection, organizations would have to pay extremely high prices as fines. The time of protecting data and other related processes would increase the workload of the employees and it will take more time to complete the allocated tasks. Training is a vital element of grooming employees to become better. When an organization pursuing a journey of establishing a data protection culture, without even knowing, the company might go to an extreme level of arranging more pieces of training. However, extensive pieces of training may bring negative impacts to the organizations compared to the benefits. There could be instances where certain pieces of training could be irrelevant. Then employees might not take these pieces of training seriously and positively.

III. Methodology

This study focuses on the issues of individual data privacy breaches and being non-compliant to various data protection regulations in both local and global companies and human resources responsibility to make it compliant. Though data privacy might apply to many industries, this study gives special reference to the BPM industry which is one of the main industries which liaise with data processing and data managing. Another important aspect of being in the business process management industry is that company has to be compliant with a lot of strict foreign data protection regularities such as GDPR in the European Union (EU) where data breach would cost extremely high fines.

This study is predominantly designed as a qualitative study based on the constructivist paradigm, to identify the role of human resource professionals in ensuring data protection. The study attracted respondents from a variety of different backgrounds as human resource professionals and employees who works in the BPM industry. In this study, both human resource professionals and other employees' perspectives on data protection were considered.

Both Primary and Secondary data has been utilized in the current study. Primary data has been collected through one to one interviews with the target group of six human resource professionals in the BPM industry.

Table 4.1: Respondent Demographics

Respondent	Company	Position	Age
1	A	Manager – HR	38
2	B	Group Manager – HR	36
3	C	Deputy Manager - Learning	32
4	D	General Manager – HR	45
5	A	HR Executive – HR	29
6	C	Recruitment Analysis - HR	26

Source: Personal Interview Data (2020)

Further forty employees were interviewed through two equal focus group interviews to understand the perception of human resources professionals' commitments towards individual data protection.

Moreover, Secondary data was extracted from internal policies, newspaper articles, researches, and websites. Secondary sources including data policy and legal documents were used to understand the applicable law for data protection. Collected data was analyzed and represent graphically.

IV. Data Analysis and Discussion

BPM industry professionals stressed that they have proper ethics, policies, and regulations on data protection since they are serving global clients. There were six human resource professionals, all agreed that they have data protection policies and adhering to GDPR. Further, they are more concerned about storing personal data, processing, and disseminating among relevant parties.

Human resources professionals were given an adequate commitment to ensuring data protection and avoid any possible data breaches in the organization. The respective areas were availability of a data protection policy, access levels to the data, appropriate consent from employee or client, processes to support the data protection, keeping a track of security incidents, privacy by design in the systems, what actions to be taken during a data breach, mechanism of delete the data based on the request. The highest positive rating was received for the content of, *'Is access to data given on a need-to-know basis in your company?*'. This means that every company ensures that all staff is just not given access to all the data

Respondent 2 mentioned that there are precautions that we can take when we design the human resource information systems *"There are mechanisms that we can use to apply technology to resolve data protection issues"*. Most of the BPM organizations have standard consent papers when they collect information from employees and clients. This has been manifested as *"According to GDPR guidelines we need to provide consent papers when collecting personal data from relevant parties"* from respondent 1, 2, 4, 5, and 6.

> *"Data protection is paramount important to every organization now more than ever before. It's not only the IT department but the*

communication and collaboration should be started from human resources professionals and steer the journey of becoming an organization where data protection is given utmost importance. Though there are multiple challenges, this cultural change is essential for any organization to survive in the future global competition."

Participant 4

Data protection can ensure through proper encryption. Content analysis on encrypted data transmission, processes to support the data protection, keeping a track of security incidents, privacy by design in the systems, and mechanism of delete the data based on the request were received doubtful feedback. On the other hand, questions on access to data given on a need-to-know basis, encrypted data transmission, processes to support the data protection, have received zero negative feedback. It means most of the organizations have those security checks in place towards data privacy. Finally, the areas organizations need to give focus on are sensitive data encrypted especially during transferring and storing and updating privacy notices and privacy policies. Both these areas have been rated negatively as 56% each with 'no' answer.

Organizations take many precautions to ensure individual data protection. Though BPM organizations ensure data protection, based on the focus group interviews, employees feel their data is unprotected. Based on the focus group interviews, employees' trust in the commitment of the human resources towards ensuring data protection and data processors in the organization are sound with their responsibilities on data privacy. Employees were doubtful data privacy up to a certain extend. Three-quarters of the participants were unaware of 'Do you have a policy on data protection in your organization?', 'Do you have a 'clean desk' policy in your organization? , and 'Is there an identifiable person in your organization who is responsible for the data protection in your company?. These doubtful answers imply that the staff is not aware of provisions available in their organizations about data privacy. All in all most of the employees who are working in the BPM industry are not positively answered and their responses indicate that there should be more awareness to be done on the subject of data protection.

V. Conclusion

The human resources role has constantly changed in recent years moving away from an administrative role in the past. The new trends in data protection and privacy laws. This study shows how ready Sri Lankan human resources professionals and what are the actions they should take in their respective areas to be compliant with data integrity and individual data privacy issues [11]. Employees feel more secure and protected when they know that the organization follows on the data protection principles and rules to protect their data.

Individual data security indirectly impacts to increase organizational performance, productivity. It creates a committed and long-term relationship with mutual trust and support between employee and employer in the long run. Further, human resource professionals need to work also in collaboration with other functions such as IT and risk management and legal teams, opening a dialogue up with colleagues regarding data protection and embracing the appropriate technologies.

VI. Recommendations

One of the major concerns that employees have on data protection is whether the organization would delete the data after they exit from the company. Similarly, candidates are not sure how long would the organization would retain the data with them. Most of the human resources professionals are failed to address these concerns. Though there is a very organization that has a specific hiring policy that would state they will delete the candidate data after 6 months, none of the organizations confirmed the fact on employee data would be deleted after a particular period.

On the other hand, clients also have a valid concern about how long the organization would retain their data with the organizations. If an organization has a clear declaration that they would delete the data as per a data retention schedule and the mechanism of destroying such data, that would be a great plus point for the organizations to win the trust of candidates, employees, or clients.

This should be done in two-way communication. For employees, at the time of recruitment, they should be clearly informed on the reasons why the organization requires certain individual data and very clearly communicate all types of policies including data protection, privacy policy, data breach reporting policy, access control policy, and data retention policy. Also, they should be communicated on the changes to such policies and should obtain employee's consent.

The consent from employees or clients should not be ambiguous and general. It should be obtained specifically mentioning the reasons and should be specific in nature. Also, when obtaining consent there should be a mechanism for employees to request not to retain certain confidential data. For organizational benefit, employees should be given adequate pieces of training and awareness on data protection and cybersecurity breaches. This will help the organization to handle data privacy and data protection proactively. Another progressive step towards the data protection culture is appointing a specific person to handle data protection. Most of the large organizations would have a dedicated person purely for this reason.

Finally, the organizational information technology infrastructure should allow the organization to be compliant with the required regulatory standards. This includes system development with privacy by design method which ensures data protection from the system design stage. System security controls, maintaining system logs, and the latest security updates.

Appendix

Employers perspective on GDPR and human resource commitment

1. Do you have a data protection policy in your organization?
2. Is sensitive data encrypted during your organization especially during transferring and storing?
3. Is access to data given on a need-to-know basis in your

company?

4. Do you have the right level of consent from employees or clients?
5. Do you have processes in place to support data access requests?
6. Are you keeping a track of security incidents such as security violations, downtimes, and updates?
7. Do you incorporate 'privacy by design' into your IT systems?
8. Do you measure data protection compliance in your organization with global data privacy regulations?
9. Do we know what actions to be taken in an impactful security breach?
10. Have you recently updated your privacy notices and privacy policies?
11. Do you have a mechanism to delete data if requested by an employee or client to do so?

Employees perspective on GDPR and human resource commitment

1. Do you know about data protection regulations?
2. Do you have a policy on data protection in your organization?
3. Do you feel that HR ensures data security and privacy in your organization?
4. Do you know that organization needs to have your consent to obtain and store your personal information?
5. Do you think the staff who are processing data in your organization are thorough with their obligations towards data protection?

ACKNOWLEDGMENT

I would like to convey my sincere gratitude to all the participants who actively given their contribution, without their participation this would have been a little success. Finally, I would like to express my gratitude to HGM Wickremeratne, the University of Colombo for given proper guidance and direction.

REFERENCES

[1] Axinte, S. D., Petrica, G., & Bacivarov, I., "GDPR impact on company management and processed data.", 19(165), 150-153, 2018.

[2] Birkhoff, A., "9 Ways the GDPR Will Impact HR Data & Analytics", Retrieved from https://www.analyticsinhr.com/blog/general-data-protection-regulation-gdpr-impact-hr-analytics/, 2018.

[3] Confessore, N., "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", Retrieved from The New York Times: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, 2018.

[4] De Soysa, S., "The right to privacy and a data protection act: Need of the hour", Colombo. Retrieved from http://www.ft.lk/article/606874/The-right-to-privacy-and-a-data-protection-act:-Need-of-the-hour, 2017.

[5] Guo, Y., Cao, L., Gao, X., & Xuming, L. V., "Understanding of the common methods in e-HRM data security," Journal of Physics, 1-6. doi:10.1088/1742-6596/1237/2/022010, 2019.

[6] Hadabas, K., "How will the GDPR affect human resources professionals?" Retrieved from https://tresorit.com/blog/how-will-the-gdpr-affect-human-resources-professionals/, 2018.

[7] Lakiara, E., & Batistic, S., "The role of data protection rules in the relationship between human resource commitment systems and employee privacy. With a special focus on Greek and Dutch corporations," Data Protection and Employees, 2018

[8] Smith, H. J., Dinev, T., & Xu, H., "Information privacy research: an interdisciplinary review." MIS Quarterly, 35(4), 989-1016, 2011.

[9] Sirur, S., Nurse, J. R., & Webb, H., "Are we there yet?: Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR).," (pp. 1-9). Retrieved from https://www.researchgate.net/publication/327160034, 2018.

[10] Xuereb, K., Grima, S., Bezzina, F., Farrugia, A., & Marano, P., "The impact of the General Data Protection Regulation on the financial services' industry of Small European States," International Journal of Economics and Business Administration, 7(4), 243-266. Retrieved from https://www.researchgate.net/publication/338007803, 2019.

[11] Žuľová, J., Švec, M., Madleňák, A., "Personality aspects of the employee and their exploration from the GDPR perspective," Central European Journal of Labour Law and Personnel Management, 1 (1), 68-77. Retrieved from https://doi.org/10.33382/cejllpm.2018.01.05, 2018.

AUTHORS

First Author – PRD Wijesingha, Post-graduate Student, Sabaragamuwa University of Sri Lanka and wijesinghedif@gmail.com
Second Author – HGM Wickremeratne, Post-graduate, University of Colombo and gayanmw@gmail.com

Correspondence Author – PRD Wijesingha, wijesinghedif@gmail.com, +94762-489495.